

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1, pp. 1-143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

The Security & Privacy Acceptance Framework (SPAF)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

Assured Autonomy Survey

Christopher Rouff and Lanier Watkins

ISBN: 978-1-68828-078-5

now Publishers Inc.

PO Box 1024

Hardware, Platform Security for Mobile Devices

Hanover, MA 02339

Lachlan J. Gunn, N. Asokan, Jan-Erik Ekberg, Hans Liljestrand, Vi-

Jayaram Nayan and Thomas Nyman

www.nowpublishers.com

ISBN: 978-1-68083-976-0

sales@nowpublishers.com

Outside North America:

now Publishers Inc.

Cloud Computing Security: Foundations and Research Directions

Arno C. Korb, Reza Curtmola, Jonathan Katz, Jason Nieh, Ahmad-

Reza Sadeghi, Radu Sion and Yinqian Zhang

The Netherlands

ISBN: 978-1-68083-958-6

Tel. +31-6-51115274

The preferred citation for this publication is

Expressing Information Flow Properties

S. Das et al. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations

and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1-143, 2022.

ISBN: 978-1-68083-936-4

ISBN: 978-1-63828-119-1

© 2022 S. Das et al.

Accountability in Computing: Concepts and Mechanisms

Joan Feigenbaum, Aaron D. Jaggard and Rebecca N. Wright

ISBN: 978-1-68083-784-1

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

The Security & Privacy Acceptance Framework (SPAF)

Published, sold and distributed by:

now Publishers Inc.

PO Box 1024

Hanover, MA 02339

United States

Tel. +1-781-985-4510

www.nowpublishers.com

sales@nowpublishers.com

Outside North America:

now Publishers Inc.

PO Box 179

2600 AD Delft

The Netherlands

Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1-143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

Sauvik Das
Carnegie Mellon University
sauvik@cmu.edu

Cori Faklaris
University of North Carolina
cfaklari@unc.edu

Jason I. Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

Laura A. Dabbish
Carnegie Mellon University
dabbish@cs.cmu.edu

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder, the essence of knowledge Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

now

the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

Volume 5, Issue 1-2, 2022

Editorial Board

Published, sold and distributed by:

now Publishers Inc.

Editors-in-Chief

Anupam Datta

Hanover, MA 02339

United States

Tel. +1-781-985-4510

Editors
www.nowpublishers.com

sales@nowpublishers.com

Martin Abadi

Outside North America
Google and University of California,

San Francisco, CA, USA

PO Box 179

Michael Backes

2600 AD Delft

Soarland University

The Netherlands

Dan Boneh

Stanford University, USA

The preferred citation for this publication is

Veronique Cortier

S. Das et al.

Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1-143, 2022.

©2022 S. Das et al.

Microsoft Research

Virgil Gligor

Carnegie Mellon University

Jean-Pierre Hubaux

APRIL rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Jeannette Wing

Columbia University, USA

Deirdre Mulligan

University of California, Berkeley

Andrew Myers

Cornell University

Helen Nissenbaum

New York University

Michael Reiter

University of North Carolina

Shankar Sastry

University of California, Berkeley

Dawn Song

University of California, Berkeley

Daniel Weitzner

Massachusetts Institute of Technology

Foundations and Trends® in Privacy and Security

Topics

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

Published, sold and distributed by:

now Publishers Inc.

PO Box 1024

• Hanover, MA 02339

United States

Tel. +1 781-985-4510

www.nowpublishers.com

• sales@nowpublishers.com

• security and privacy

Outside North America:

now Publishers Inc.

• PO Box 179

2600 AD Delft

The Netherlands

• Tel. +31 6 51115374

• The present distributed system has its publication

• privacy

• S. Das *et al.*, *The Security & Privacy Acceptance Framework (SPA-F)*, Foundations and Trends in Privacy and Security, vol. 5, no. 1-2, pp. 1-143, 2022.

• Embedded systems security; and

• privacy

• ISBN: 978-1-63828-119-1

• © 2022 S. Das *et al.*

• Hardware security

• Human factors in security and privacy

• Information flow

• Intrusion detection

• Malware

• Metrics

• Mobile security and privacy

• Language-based security and privacy

• Network security

• Privacy-preserving systems

• Protocol security

• Security architectures

• System security

• Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2022, Volume 5, 4

issues. ISSN paper version 2474-1558, ISSN online version 2474-1566.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission of the publishers.

Also available as a combined paper and online subscription.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

Contents

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands

1	Introduction	2
2	The background for this publication is	7
2.1	Models of human behavior	9
2.2	Models of technology adoption, diffusion, acceptance and privacy	14
ISBN: 978-1-63828-119-1		
3	The Security & Privacy Acceptance Framework	19
3.1	Why do we need a framework specific to S&P acceptance?	19
3.2	Awareness	22
3.3	Motivation	28
3.4	Ability	34
3.5	Summary	39
4	Encouraging Widespread Security & Privacy Acceptance	40
4.1	Improving Awareness	43
4.2	Improving Motivation	52
4.3	Improving Ability	66
5	Discussion	89
5.1	Summary of the SPAF	89
5.2	Using the SPAF: Gaps and opportunities for future research	92

now Publishers Inc. has an exclusive license to publish this material and any permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

5.2. What else matters beyond in-group and user S&A acceptance? 103

6 Conclusion **111**

Acknowledgments **114**

distributed by:

now Publishers Inc.

PO Box 1024

Hanover, MA 02339

United States

Tel. +1-781-985-4510

www.nowpublishers.com

sales@nowpublishers.com

Outside North America:

now Publishers Inc.

PO Box 179

2600 AD Delft

The Netherlands

Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

The Security & Privacy Acceptance Framework (SPAF)

Sauvik Das¹, Cori Faklaris², Jason I. Hong¹ and Laura A. Dabbish¹

Published online and distributed by, USA; sauvik@cmu.edu,
now Publishers Inc.
jasonh@cs.cmu.edu, dabbish@cs.cmu.edu
PO Box 1024

¹University of North Carolina, Charlotte, USA; cori@corifaklaris.com
Hanover, MA 02339

United States

Tel. +1-781-985-4510

www.nowpublishers.com

sales@nowpublishers.com

Outside North America:

How can we encourage end-user acceptance of expert recommended cybersecurity and privacy (S&P) behaviors? We

present a review of prior art in human-centered S&P and identified three

barriers to end-user acceptance of expert recommendations:

(1) awareness: i.e., people may not know of relevant security

threats and appropriate mitigation measures; (2) motivation:

people may not know when, why, and how to effectively

implement S&P behaviors. These three barriers make up

what we call the “Security & Privacy Acceptance Framework”

(SPAF). We then review and critically analyze prior work

that has explored mitigating one or more of the barriers

that make up the SPAF. Finally, using the SPAF as a lens,

we discuss how the human-centered S&P community might

be oriented to encourage widespread end-user acceptance of

S&P behaviors by employing integrative approaches

that address each one of the awareness, motivation, and

ability barriers.

For those organizations that have been granted a photocopy license, a separate system of payment

has been arranged. Authorization does not extend to other kinds of copying, such as that for

general distribution, for advertising or promotional purposes, for creating new collective works, or

for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright

owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781

871 0245; www.nowpublishers.com; sales@nowpublishers.com

Sauvik Das, Cori Faklaris, Jason I. Hong and Laura A. Dabbish (2022), “The Security

and Privacy Acceptance Framework (SPAF) Publication and Trends in Privacy

and Security, Vol. 7, No. 1-2, pp. 1-143, DOI:10.1561/3300000026

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

© 2022 S. Das et al.

Foundations and Trends[®] in Privacy and Security 1

Introduction

Published, sold and distributed by:

now Publishers Inc.

PO Box 1024

Hanover, MA 02339

United States

Tel. +1-781-985-4510

www.nowpublishers.com

sales@nowpublishers.com

Outside North America:

now Publishers Inc.

PO Box 179

2600 AD Delft

The Netherlands

Tel. +31-6-51115274

Cybersecurity and privacy (S&P) unlock the full potential of computing. Use of encryption, authentication, and access control, for example, allows employees to correspond with professional colleagues via email with reduced fear of leaking confidential data to competitors or cyber-criminals, parents to share photos of children with remote loved ones over the Internet with reduced fear of this data reaching the hands of unknown strangers, and anonymous whistleblowers to share information about problematic practices in the workplace with reduced fear of being outed. Conversely, failure to employ appropriate S&P measures can leave people and organizations vulnerable to a broad range of threats.

In short, the security and privacy decisions we make on a day-to-day basis determine whether the data we share, manipulate, and store online is protected from theft, surveillance, (and) exploitation. It is unsurprising, therefore, that the compromising of weak security and privacy practices for those organizations that have been granted a photocopy license, a separate system of payment for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc. at PO Box 1024, Hanover, MA 02339, USA, Tel. +1-781-871 0245; www.nowpublishers.com; sales@nowpublishers.com of protecting digital resources and data from intruders. Cybersecurity is commonly abbreviated to just as security and used in addition to this acronym we use S&P as a shorthand for "cybersecurity and privacy." We use this short-hand in various ways, typically as a descriptor: e.g., S&P threats, S&P behaviors, and S&P tools.

Foundations and Trends® in Privacy and Security



Figure 1.1: Cybercrime is estimated to cause over \$1 trillion USD in damages to the global economy, and much of it is enabled by human error. Yet, user acceptance and adoption of expert-recommended security and privacy behaviors remains low. There remains an immense opportunity for impact by improving end-user acceptance and adoption of expert-recommended security and privacy behaviors.

Outside North America:

now Publishers Inc.
 PO Box 1024
 Hanover, MA 02339
 United States
 Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Many of the data breaches that are responsible for these damages involve human error or manipulation — i.e., improperly configured security settings, the accidental divulsion of key account credentials, or the unwitting installation of destructive malware. Moreover, as an increasing share of economic and social activity is conducted partially or exclusively online, the ramifications of these breaches have never been more significant. In 2021, for example, a ransomware attack crippled the Colonial Pipeline company, causing gas outages all over the eastern seaboard of the United States, resulting in outages, panic and predatory price inflation — and all because the company’s private VPN was accessible without multi-factor authentication (Kellner, 2022). The Colonial Pipeline company incident is not an isolated incident. In early 2013, the Associated Press’s Twitter account was compromised through a password phishing scheme, and erroneously tweeted that President Obama was injured in a bombing (Moore and Roberts, 2013). In response, stock prices plummeted, adversely affecting thousands. The cause? The AP’s Twitter account credentials were phishing, and the account was not protected with two-factor authentication. More generally, in 2020, Verizon published an analysis of 3950 security incidents, showing that the most common actions that led to breaches were social attacks to use this content may be obtained from the copyright license holder. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 985-4510; www.nowpublishers.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 985-4510; www.nowpublishers.com

© 2022 S. Das et al.

Foundations and Trends in Privacy and Security

type that is consistently increasing year to year in frequency is [human] error.” (Verizon, 2020). The 2022 version of that report estimated that the “human element” drove 82% of the 5212 breaches studied (Verizon, 2022). Unsurprisingly, prior work has found that the S&P behaviors that experts recommend only thinly overlap with the behaviors that people find important and adopt (Ion *et al.*, 2015; Busse *et al.*, 2019). The Massachusetts Institute of Technology (MIT) researchers found that if enough people employed basic, expert-recommended best practices — e.g., keeping one’s software up-to-date, using multi-factor authentication on important accounts, using a password manager to ensure the reliable use of strong, random passwords unique for each individual account — the cybercrime industry would be hamstrung. The researchers estimated that such attacks would be substantially increased, shifting economic incentives, and would likely reduce the prevalence of all but the most sophisticated, targeted attacks. Yet, despite decades of improvements to the usability of S&P systems, end-users still struggle with adopting expert-recommended S&P practices. Indeed, as of early 2018, fewer than 10% of Google account holders had enrolled in two-factor authentication, and a similar 7% of Google users reused their account passwords (Milka, 2018). Recent Pew surveys found that only 12% of Internet users in the U.S. use password managers and only 44% immediately update the operating system on their mobile phones (Olmstead and Smith, 2017).

This discrepancy — between the massive damages caused by the exploitation of weak security behaviors, and the existence of security technologies that can significantly reduce these damages, as summarized in Figure 1 — brings the question: “How can we encourage end-users to heed the advice of S&P experts?” Put another way, we might ask: “What inhibits acceptance of appropriate S&P behaviors among end-users, and how can we overcome those inhibitors?”

In this monograph, we conducted an extensive review of prior literature for those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Haverhill, MA 02339, USA; Tel: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to extend this material into other media is granted by now Publishers Inc. Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Haverhill, MA 02339, USA; Tel: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

and behavioral economics. We start with a comprehensive review of existing models of human behavior and technology adoption and use these models as a lens to contextualize prior findings in human-centered

Foundations and Trends® in Privacy and Security is less straightforward from the perspective of end-user action — indeed, placing the onus strictly on end-users is a problematic approach. For these situations, there may be a stronger need for regulation of bad-faith corporate and intelligence agency practices, rather than targeted design interventions and behavioral improvements on the part of end-users.

Published, sold and distributed by:
now Publishers Inc.

PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

References

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179

2600 AD Delft
The Netherlands
J. A. Halderman, J. Hoffman-Andrews, J. Kasten, E. Rescorla, *et al.* (2019). “Let’s Encrypt: an automated certificate authority to encrypt the entire web”. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*: 2475–2487. ISBN: 978-1-63828-119-1

S. Das *et al.* (2022). “The Security & Privacy Acceptance Framework (SPA-F): Foundations and Trends” in *Privacy and Security*, vol. 5, no. 1-2, pp. 1–143, 2022.

Acar, Y., S. Fahl, and M. L. Mazurek. (2016). “You are not your developer, either: A research agenda for usable security and privacy research beyond end users”. *2016 IEEE Cybersecurity Development (SecDev)*: 3–8.

Ackerman, M. S. (2000). “The intellectual challenge of CSCW: the gap between social requirements and technical feasibility”. *Human-Computer Interaction*, 15(2-3): 179–203.

Acquisti, A., I. Arjeric, R. Balebako, L. Brandimarte, L. F. Cranor, S. Kumar, and P. G. Leon. N. Satchi, T. Seniar, M. Sleeper, *et al.* (2017). “Nudges for privacy and security: Understanding and assisting users’ choices online”. *ACM Computing Surveys (CSUR)*, 50(3): 1–41.

Acquisti, A., L. Brandimarte, and G. Loewenstein. (2015). “Privacy and human behavior in the age of information”. *Science*, 347(6211): 309–317.

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale.

In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 3095.

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 3095.

Published online first in *Foundations and Trends in Privacy and Security*, 3(1): 26–33, 2022.

© 2022 S. Das *et al.*

© 2022 S. Das *et al.*

© 2022 S. Das *et al.*

© 2022 S. Das *et al.*

© 2022 S. Das *et al.*

- Foundations and Trends in Privacy and Security (2009). “User-centered security in communications of the ACM (CACM). 42(12): 40–46. DOI: [10.1145/322796.322806](https://doi.org/10.1145/322796.322806).”
- Addae, J. H., M. Brown, X. Sun, D. Towey, and M. Radenkovic. (2017). “Measuring attitude towards personal data for adaptive cybersecurity. Published, sold, and distributed by: now Publishers Inc. Information & Computer Security. Aizenbox 1024 (1991). “The theory of planned behavior”. *Organizational Behavior and human decision processes*. 50(2): 179–211. Hanover, MA 02339 United States
- Akhtaw, D. and A. P. Felt. (2013). “Alice in warningland: a large-scale field study of browser security warning effectiveness”. In: *Proc. of the ACM on Security and Privacy*. 2013, 257–272. ISBN: 978-1-4553-5913-9
- Alter, M. A., J. Godfrey, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski. (2022). “From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals?” *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW15): 71–28. ISBN: 978-1-59593-714-1
- Almubinedi, H. F., Schaub, N., Sadeh, I., Adjerid, A., Acquisti, J., Gluck, L. F., Cranor, and Y. Agarwal. (2015). “Your location has been shared 5,398 times! A field study on mobile app privacy nudging”. In: *Proceedings of the 33rd annual ACM conference on human factors and ergonomics*. 2012, 787–796. ISBN: 978-1-4553-5913-9
- Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2016). “A review of using gaming technology for cybersecurity awareness”. *Int. J. Inf. Secur. Res. (IJISR)*. 6(2): 660–666.
- Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2017). “Enhancing cyber security awareness with mobile games”. In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITSS)*. IEEE, 129–134. Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 per copy is paid directly to CCC. This service for users can be found on the internet at: www.copyright.com
- Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2017). “Design and evaluation of an augmented reality game for cybersecurity awareness (cybar)”. For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc. 2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems. IEEE, 125–128. ISBN: 978-1-4222-1251-2
- Alotaibi, F., A. and A. S. Saddik. (2006). “A novel 3D graphical password schema”. In: *2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems*. IEEE, 125–128. ISBN: 978-1-4222-1251-2
- Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2017). “Enhancing cyber security awareness with mobile games”. In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITSS)*. IEEE, 129–134. Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 per copy is paid directly to CCC. This service for users can be found on the internet at: www.copyright.com
- For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc. 2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems. IEEE, 125–128. ISBN: 978-1-4222-1251-2
- Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2017). “Enhancing cyber security awareness with mobile games”. In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITSS)*. IEEE, 129–134. Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 per copy is paid directly to CCC. This service for users can be found on the internet at: www.copyright.com
- For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc. 2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems. IEEE, 125–128. ISBN: 978-1-4222-1251-2

Foundations and Trends in Privacy and Security

- Fluhrer, T. A., A. H. S. Chan, and J. K. (2008). “Thresholding: A password for more secure authentication”. *IEEE Transactions on Instrumentation and Measurement*. 57(9): 1929–1938.
- Anderson, B. B., C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. (2015). “How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study”. In: *Proceedings of the 33rd ACM conference on human factors in computing systems*. Hanover, MA, USA, 2015. pp. 283–292.
- Assal, H., and S. Chiasson. (2019). “‘Think secure from the beginning’ A Survey with Software Developers”. In: *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.
- Austin, B., I. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Orszag. (2019). “Americans and privacy: Concerned, confused and feeling lack of control over their personal information”. *Pew Research Center Internet, Science & Tech (blog)*. November. 15: 2019.
- Azencroft, S., J. Rector, R. Ladner, and J. Wobbrock. (2012). “Pass-Clouds: secure multi-factor authentication for blind people”. In: *Proceedings of the 14th international ACM SIGACCESS conference on S. Das et al.: The Security & Privacy Acceptance Framework (SPAF), Foundations and Trends in Computers and Usability*. 159:166, pp. 1–143, 2022.
- Bada, M., A. M. Sasse, and J. R. Nurse. (2019). “Cyber security awareness campaigns: Why do they fail to change behaviour?” *arXiv preprint arXiv:1901.02672*.
- Bai, W., D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. (2017). “Balancing security and usability in encrypted email”. *IEEE Internet Computing*, 21(3): 30–38.
- Barbosa, N. M., J. M. Hayes, and Y. Wang. (2016). “UniPass: design and evaluation of a smart device-based password manager for visually impaired users”. In: *Proceedings of the 2016 ACM international joint conference on pervasive and ubiquitous computing*. 49–60.
- Bauer, L., L. F. Cranor, M. K. Reiter, and K. Vaniea. (2007). “Lessons learned from the deployment of a smartphone-based access control system”. In: *Proceedings of the 3rd Symposium on Usable Privacy and Security*. 64–75.

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

- Chen, F., C. Truira, and S. Schechter. (2013). “Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore”. In: *Proc. SOUPS’13*.
- Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.
- Buchanan, T., C. Paine, A. N. Joinson, and U.-D. Reips. (2007). “Development of measures of online privacy concern and protection for use on the Internet”. *Journal of the American society for information science and technology*. 58(2): 157–165.
- Burrows, J. and T. Gebru. (2018). “Gender shades: Intersectional accuracy disparities in commercial gender classification”. In: *Conference on fairness, accountability and transparency*. PMLR. 77–84.
- Dass, S., K. J. Schäfer, and M. Smith. (2019). “Replication: no one can hack my mind revisiting a study on expert and non-expert security practices and advice”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.
- S. Das et al.: *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Security and Privacy, vol. 14, no. 1, pp. 1–43, 2019.
- “Hello AI: uncovering the onboarding needs of medical practitioners”. ISBN: 978-1-4582-9119-1.
- © 2020 Shantanu. “AI collaborative decision-making”. *Proceedings of the ACM on Human-computer Interaction*. 3(CSCW): 1–24.
- Carre, J. R., S. R. Curtis, and D. N. Jones. (2018). “Ascribing responsibility for online security and data breaches”. *Managerial Auditing Journal*.
- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.
- Chandrasekaran, V., C. Ge, B. Pang, K. Pawaz, S. Jha, and S. Banerjee. (2020). “Face-off: Adversarial face obfuscation”. *arXiv preprint arXiv:2003.08861*.
- Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 per copy is paid directly to CCC. For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., P.O. Box 1024, Hanover, MA 02331, USA. Tel. +1 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Chatterjee, R., P. Doerder, H. Orgad, C. Hawron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. (2018). “The spyware used in intimate partner violence”. In: *2018 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 741–758.
- Chen, F., M. Stewart, Z. Bai, E. Chen, L. Dabish, and J. Hammer. (2020). “Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game”. In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 1737–1749.

Foundations and Trends in Privacy and Security

- Taylor, and T. Goldstein. (2021). “LowKey: leveraging adversarial attacks to protect social media users from facial recognition”. *arXiv preprint arXiv:2101.07922*.
- Chesney, B. and D. Citron. (2019). “Deep fakes: A looming challenge for privacy, democracy, and national security”. *Calif. L. Rev.* 107: 1673–1753.
- Chowdhury, M. M., M. LaPerriere, Z. Aljallad, J. Kropczynski, H. Lipson, and P. J. Wisniewski. (2019). “Co-designing for community oversight: Helping people make privacy and security decisions together”. *Proceedings of the ACM on Human-Computer Interaction*. 3(CSCW): 1–31.
- Cranor, L. F. (1987). *Influence*. Vol. 3. A. Michel Port Harcourt. PO Box 179, 2600 AD Delft, The Netherlands.
- Costanza, C., S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Nellore. (2018). “Phishy—a serious game to train enterprise users on phishing awareness”. In: *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*. 169–181.
- S. Das et al.: *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Security and Privacy, 2021, 2021.
- Costanza, C., S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Nellore. (2018). “Phishy—a serious game to train enterprise users on phishing awareness”. *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*. 169–181.
- S. Das et al.: *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Security and Privacy, 2021, 2021.
- © 2022 Design Research Society.
- Cranor, L. F. (2008). “A framework for reasoning about the human in the loop”.
- Cranor, L. F. (2003). “P3P: Making privacy policies more useful”. *IEEE Security & Privacy* 1(6): 50–55.
- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.
- Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. For all other use, permission should be sought from Cambridge University Press, The Edinburgh Building, Shaftesbury Road, Cambridge CB2 2RU, UK, or in the USA from Cambridge University Press, 32 Avenue of the Americas, New York, NY 10013-2473, USA. The copyright in this journal is held by Cambridge University Press, and this journal is registered with the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. The copyright for users in the USA is held by the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. The copyright for users in the rest of the world is held by Cambridge University Press. The copyright for users in the rest of the world is held by Cambridge University Press.
- For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., P.O. Box 102C, Hanover, MA 01839, USA. Tel: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Das, S. (2016). “Social cybersecurity: Understanding and leveraging social influences to increase security sensitivity”. *Information Technology and e-Business Management* 17(3): 35–46.
- Das, S. (2016). “Social cybersecurity: Understanding and leveraging social influences to increase security sensitivity”. *Information Technology and e-Business Management* 17(3): 35–46.

- Das, S. (2017). “Social and Cultural Influences on Privacy and Security: An Empirical Understanding of Human Social Behavior”. *PhD thesis*. Carnegie Mellon University.
- Das, S., L. A. Dabbish, and J. I. Hong. (2019a). “A Typology of Perceived Triggers for End-User Security and Privacy Behaviors”. Published, sold and distributed by: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. PO Box 179, 2600 AD Delft, The Netherlands. 97–115.
- Das, S., M. Hayashi, and J. I. Hong. (2013). “Exploring capturable everyday memory for autobiographical authentication”. In: *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. 211–220.
- Das, S., J. Hong, and S. Schechter. (2016). “Testing Computer-Aided Memorization and Feedback for Fast Memorization of High-Value Secrets”. In: *2016 Usable Security (USEC) Workshop*. 2600 AD Delft, The Netherlands. 1–6.
- Das, S., T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. (2014a). “The effect of social influence on security sensitivity”. In: *10th Symposium on Usable Privacy and Security (SOUPS 2014)*. 143–157.
- Das, S., A. D. Kramer, L. A. Dabbish, and J. I. Hong. (2014b). “In-Credible Security and Sensitivity With Social Proof: A Large-Scale Experimental Confirmation”. In: *Proceedings of the 2014 ACM Conference on Computer and Communications Security (CCS '14)*. New York, New York, USA: ACM Press. 739–749. DOI: [10.1145/2660267.2660271](https://doi.org/10.1145/2660267.2660271).
- Das, S., A. D. Kramer, L. A. Dabbish, and J. I. Hong. (2015). “The role of social influence in security feature adoption”. In: *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 1416–1426.
- Das, S., G. Laput, C. Harrison, and J. I. Hong. (2017). “The Impact of Socially Inclusive Local Group Authentication through Shared Secret Knocks”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 304–317.
- Das, S., L. A. Dabbish, and J. I. Hong. (2018). “Breaking: A Typology of Security and Privacy News and How It’s Shared”. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1111–1126.
- Das, S., L. A. Dabbish, and J. I. Hong. (2019b). “A Typology of Perceived Triggers for End-User Security and Privacy Behaviors”. In: *Proceedings of the 2019 ACM Conference on Computer and Communications Security (CCS '19)*. New York, New York, USA: ACM Press. 1111–1126. DOI: [10.1145/3173574.3173575](https://doi.org/10.1145/3173574.3173575).

Foundations and Trends® In Privacy and Security

palace: Exploring visual-spatial paths for strong, memorable, infrequent authentication”. In: *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*. 1109–1121.

Davis, F. D. (1989). “Perceived usefulness, perceived ease of use, and user acceptance of information technology”. *MIS quarterly*: 319–340. Published, sold and distributed by: now Publishers Inc.

Domingo, A., A. Lerner, A. Shostack, and T. Kohno. (2013). “Control: The design and evaluation of a card game for computer security awareness and education”. In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 915–928. www.nowpublishers.com/sales@nowpublishers.com

Dhanji, R. J. D., Tygar, and M. Hearst. (2006). “Why phishing works”. *CHI '06*. No. April. New York, New York, USA: ACM Press. 581–590. DOI: [10.1145/1124772.1124861](https://doi.org/10.1145/1124772.1124861).

Dinic, P. and P. Dourish. (2005). “Social navigation as a model for user security”. In: *Proc. SOUPS '05*. New York, New York, USA: ACM Press. 101–108. doi: [10.1145/1073001.1073011](https://doi.org/10.1145/1073001.1073011).

Distler, V., G. Lenzi, C. Lallemand, and V. Koenig. (2020). “The framework of privacy and security enhancing fiction: How 4D zoom help users be more secure”. In: *New security paradigms workshop 2020*. ISBN: 978-1-5386-19-1-1 © 2023-58 Das et al.

Do, Y., L. T. Hoang, J. W. Park, G. D. Abowd, and S. Das. (2021a). “Spidey Sense: Designing Wrist-Mounted Affective Haptics for Communicating Cybersecurity Warnings”. In: *Designing Interactive Systems Conference 2021*. 125–137.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1031, Hanover, MA 02339, USA. Tel: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

Do, Y., L. T. Hoang, J. W. Park, G. D. Abowd, and S. Das. (2021b). “Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust”. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 5(4): 1–21.

Do, Y., L. T. Hoang, J. W. Park, G. D. Abowd, and S. Das. (2021c). “Bit Whisperer: Improving Access Control over Ad-hoc, Short-range, Wireless Communications via Surface-bound Acoustics”. In: *Proceedings of the 34th ACM User Interface Software and Technology Symposium (UIST)*. Use apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

- user security awareness”. *computers & security*. 26(1): 73–80.
- Dourish, P. and K. Anderson. (2006). “Collective information practice: Exploring privacy and security as social and cultural phenomena”. *Human-computer interaction*. 21(3): 319–342.
- Published, sold and distributed by:
Dourish, P., R. E. Grinter, J. Delgado de la Flor, and M. Joseph. (2004). PO “Security in the wild: user strategies for managing security as an Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
- Dourish, P. and F. Khan. (2018). “Effects of peer feedback on password sales@nowpublishers.com
strongly”. In: *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–9.
- Edwards, W. R., E. S. Poole, and J. Stoll. (2008). “Security automation PO Box 179
considered harmful?” In: *Proceedings of the 2007 Workshop on New 2600 AD Delft
Security Paradigms*. 33–42.
- Egelman, S., D. Molnar, N. Christin, A. Acquisti, C. Herley, and S. Krishnamurthi. (2010). “Please Continue to Hold: An empirical study on user tolerance of security delays”. In: *Proc. WEIS’10*. URL: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.167.5560>.
- Egelman, S. and E. Peer. (2015a). “Scaling the security wall: Developing a security behavior intentions scale (sebis)”. In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA. Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Egelman, S. and E. Peer. (2015b). “The myth of the average user: Improving privacy and security systems through individualization”. In: *Proceedings of the 2015 New Security Paradigms Workshop*. 16–28. now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

Herley, C. (2013). “Does my password go up to eleven? The impact of password meters on password selection”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2379–2388.

Published, sold and distributed by:

now Publishers Inc.
PO Box 924
Hanover, MA 02339
United States

Faklaris, C. (2022). “Toward a Socio-Cognitive Stage Model of Cyberspace Security Behavior Adoption”. *PhD thesis*. US National Science Foundation.
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Dabbish, L. A., Dabbish, L. A., and J. I. Hong. (2022). “Do They Accept or Resist Cybersecurity Measures? Development and Validation of the US Italian Security Attitude Inventory (SA-13)”. *arXiv preprint arXiv:2204.03114*.
Faklaris, C., L. A. Dabbish, and J. I. Hong. (2019). “A Self-Report Measure of End-User Security Attitudes (SA-6)”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 61–77.

Karimi, A. Shah, B. Subramanian, and S. Das. (2020). “Blind and Human: Exploring More Usable Audio CAPTCHA Designs”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 111–125.
S. Das et al. “The Security & Privacy Acceptance Framework (SPAFA). Foundations and Trends in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

Chen, J., Mendelsohn, J., Bassen, J., and M. S. Bernstein. (2018). “A Conversational agent for complex tasks”. In: *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–12.

Felt, A. P., A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettet, H. Harris, and J. Grimes. (2015). “Improving SSL warnings: User comprehension and adherence”. In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2893–2902.

Rek, A. P., R. W. Reeder, H. Alammeh, and S. Consolvo. (2014). “Experimenting at scale with google chrome’s SSL warning”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2601–2610.

Ferguson, A. J. (2009). “Fostering e-mail security awareness”. *The West Point carbonate*. *Edutec Quarterly*. 28(1): 54–57.

Fishbein, M. (1979). “A theory of reasoned action: some applications and implications”.
now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this material must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security (formerly Foundations and Trends in Security and Privacy) (2019). “Behavioral determinants of privacy and security behavior: An introduction to theory and research”. *Philosophy and Rhetoric*. 10(2).

Fogg, B. (2009). “A behavior model for persuasive design”. In: *Proceedings of the 4th International Conference on Persuasive Technology - Published, sold and distributed by: Persuasive 09*. 1. DOI: [10.1145/1541948.1541999](https://doi.org/10.1145/1541948.1541999).

Forgot, S., Komanduri, A., Acquisti, N., Christin, L. F., Cranor, L. B., and Haner, P. (2014). “Building the security behavior observatory: An infrastructure for long-term monitoring of client machines”. In: *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*. 1. DOI: [10.1145/2533921.2533922](https://doi.org/10.1145/2533921.2533922).

Frisk, A. N., Mallin, M., Harbach, E., Peer, and S. Egelman. (2019a). “A promise: the effect of commitment devices on computer security intentions”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Frisk, A. N., Egelman, S., Bernd, J., Lee, F., Schaub, and S. Egelman. (2019b). “Privacy and security threat models and mitigation strategies of older adults”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 1-2, pp. 1–143, 2022.

Furnell, S. A., Jusch, and D. Katsabas. (2006). “The challenges of data mining and using security: A survey of end-users”. *Computers & Security*. 25(1): 27–35.

Gaw, S., E. W. Felten, and P. Fernandez-Kelly. (2006). “Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail”. In: *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI 06)*. New York, New York, USA: ACM Press, 591–600. DOI: [10.1145/1124772.1124862](https://doi.org/10.1145/1124772.1124862).

George, C., M. Khanna, D. Buschek, and H. Hussmann. (2019). “Investigating the third dimension of authentication in immersive virtual reality and in the real world”. In: *2019 IEEE Conference on Virtual Reality and User Interfaces (VR)*. 1-2, pp. 1–9.

Grecks, J. W., R. Edwards, and E. D. Myhratt. (2009). “Challenges in supporting end-user privacy and security management with social navigation”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1-2, pp. 1–12.

© 2022 by now Publishers Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service provided that the fee of \$12.00 per copy is paid directly to CCC. For those organizations that have been granted a photocopy licence by CCC, a separate system of payment has been arranged. The fee code for users of the Transactional Reporting Service is 0167-1776/2022 \$12.00. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., P.O. Box 1091, Hanover, MA 02339, USA; Tel.: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

- Older, D. M. The Foundations and Trends® in Privacy and Security (1999). “Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 109–126. Published, sold and distributed by: now Publishers Inc.
- Golla, M., G. Ho, M. Lohmus, M. Pulluri, and E. M. Redmiles. (2021). “Developers are not the enemy!: The need for usable security apis”. *IEEE Security & Privacy*. 14(5): 41–46. United States Tel. +1-781-985-4510 www.nowpublishers.com
- Guan, T. S., Farhang, Y. Pu, P. Guo, J. Grossklags, and P. Liu. (2017). “Automated Reasoning User Control for Password Managers through Out-of-Process”. In: *International Conference on Security and Privacy in Communication Systems*. Springer. 673–686. PO Box 179, 2600 AD Delft, The Netherlands Tel. +1-781-985-4510 www.nowpublishers.com
- Gubersk, T., A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and N. Schantz. (2018). “Keeping a low profile? Technology, risk and privacy among undocumented immigrants”. In: *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–15. The Netherlands Tel. +1-781-985-4510 www.nowpublishers.com
- Haber, E. and E. Kandogan. (2007). “Security administrators: A breed apart”. In: *IEEE Security & Privacy*, vol. 5, no. 1-2, pp. 1–143, 2022.
- Hagger, M. S. (2016). “Non-conscious processes and dual-process theories in health psychology”. *Health Psychology Review*. 10(4): 375–380. © 2016 now publishers
- Halperin, D., T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. (2008). “Security and privacy for implantable medical devices”. *IEEE pervasive computing*. 7(1): 30–39. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, or in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.
- Haney, Y. and S. Farman. (2021). “User Perceptions of Responsibility for Smart Home Privacy and Security”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 428–442. Published, sold and distributed by: now Publishers Inc. The services’ for users can be found on the internet at www.copyright.com
- Hang, A., A. De Luca, and H. Hussmann. (2015). “I know what you did last week do you: dynamic security questions for fallback authentication on smartphones”. In: *Proceedings of the 9th Annual ACM Conference on Human Factors in Computing Systems*. 1383–1392. For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publisher Inc., PO Box 179, 2600 AD Delft, USA Tel. +1-781-985-4510 www.nowpublishers.com
- Hans, G. S. (2012). “Privacy policies, terms of service, and FTC enforcement: Broadening unfairness regulation for a new era”. *Mich. Tech. L. Rev.* 19: 163. Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security

- inequality in skills and uses among older adults.” *Canadian Journal of Communication*. 42(2).
- Hartzog, W. and D. J. Solove. (2014). “The scope and potential of FTC data protection”. *Geo. Wash. L. Rev.* 83: 2230.
Published, sold and distributed by:
 now Publishers Inc.
 PO Box 179
 2600 AD Delft
 The Netherlands
 Tel. +1-781-985-4510
 www.nowpublishers.com
 sales@nowpublishers.com
- Hayashi, E., S. Das, S. Amini, J. Hong, and I. Oakley. (2013). “Casa: Context-aware scalable authentication”. In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. 1–10.
now Publishers, Inc.
 PO Box 179
 2600 AD Delft
 The Netherlands
 Tel. +1-781-985-4510
 www.nowpublishers.com
 sales@nowpublishers.com
- Hendriks, M., A. Al-Sherbaz, and B. Victoria. (2016). “Game based cyber security training: are serious games suitable for cyber security training?” *International Journal of Serious Games*. 3(1). DOI: [10.1145/1719030.1719050](https://doi.org/10.1145/1719030.1719050)
- Herley, C. (2009). “So long, and no thanks for the externalities”. In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Systems*. New York, New York, USA: ACM Press. 133–144. DOI: [10.1145/1719030.1719050](https://doi.org/10.1145/1719030.1719050)
- S. Das et al.: *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, 2012. DOI: [10.1561/3300000026](https://doi.org/10.1561/3300000026)
ISBN: 978-1-93825-119-1
- Herley, C. and P. van Oorschot. (2009). “Passwords: If We’re So Smart, Why Are We Still Using Them?” *Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC’09)*. DOI: [10.1007/978-3-642-03549-4_14](https://doi.org/10.1007/978-3-642-03549-4_14).
- Herley, C., P. C. Van Oorschot, and A. S. Patrick. (2009). “Passwords: All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.” In: *International Conference on Financial Cryptography and Data Security*. Springer. Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 is paid directly to CCC. For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 179, 2600 AD Delft, The Netherlands. Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Hatcher, S. (2009). “If FC is an Internet privacy norm entrepreneur, The *Vand. L. Rev.* 53: 2041.”
- For these organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 179, 2600 AD Delft, The Netherlands. Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Hübner, W., A. Samuel, Y. Yuan, H. Zhang, and S. Sajad. (2020). “Survey of serious games for cyber security education and training”. In: *Proceedings of the 2020 IEEE Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 327–346. DOI: [10.1109/SMC4310220.2020.00070458](https://doi.org/10.1109/SMC4310220.2020.00070458).
- Hunter, P., R. Reeder, and S. Consolvo. (2015). “No one can hack my mind”: Comparing Expert and Non-Expert Security Practices”. In: *Symposium on Usable Privacy and Security (SOUPS)*. 327–346. DOI: [10.1145/2731022.2731027](https://doi.org/10.1145/2731022.2731027)
now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this material must be obtained from the publisher. Please apply to now Publishers Inc., PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

- Foundations and Trends® in Privacy and Security (2007).
 “Social phishing”. *Communications of the ACM*. 50(10): 94–100.
- Jain, M., R. Tripathi, I. Bhansali, and P. Kumar. (2019). “Automatic generation and evaluation of usable and secure audio ReCAPTCHA”. In: *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*. 355–366. Publishers Inc.
- Jansson, K. and R. von Solms. (2013). “Phishing for phishing awareness”. *Behavior & information technology*. 32(6): 584–593. United States
- Jefferson, B. J. (2018). “Predictable policing: Predictive crime mapping and geographies of policing and race”. *Annals of the American Association of Geographers*. 108(1): 1–16. Publisher, Inc.
- Jin, H., G. Lin, D. Hwang, S. Kumar, Y. Agarwal, and J. Hong. (2022). “A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes”. In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. 1571–1571. Tel. +1-781-985-4510.
- Jorgensen, Z. and T. Yu. (2011). “On mouse dynamics as a behavioral biometric for authentication”. In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. Foundations and Security, vol. 5, no. 1-2, pp. 1–143, 2022. ISBN: 978-1-6328-419-4.
- Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan. ISBN: 978-1-6328-419-4.
- Kaplan, S., M. D’Arcy, C. R. Crowell, A. Striegel, and D. Van Bruggen. (2014). “An exploratory investigation of message-person congruence in information security awareness campaigns”. *Computers & security*. 43: 64–76.
- Kang, R., L. Dabbish, N. Fruchter, and S. Kiesler. (2015). “My data just goes everywhere: User mental models of the internet and implications for privacy and security”. In: *Symposium on Usable Privacy and Security (SOUPS) 2015*. 39–52. Rosemont, IL: ACM Press, 2015. ISBN: 978-1-4503-2900-9.
- Kapadia, A. G., Samjournie and R. d. Campaer. (2004). “I know why your access was denied: Regulating feedback for usable security”. In: *Proceedings of the 11th ACM conference on Computer and Communications Security*. 92–91.
- Kaplan, S. A., D. L. Vogel, D. A. Gentile, and N. G. Wade. (2012). “Increasing positive perceptions of counseling: The importance of repeated exposures”. *The Counseling Psychologist*. 40(4): 409–442. Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

- N. G. McPherson, G. H. Smith, and S. S. Scott. (2015). “A Proof: Usable Two-Factor Authentication Based on Ambient Sound”. In: *24th USENIX security symposium (USENIX security 15)*. 483–498.
- Kelley, P. G., J. Bresee, L. F. Cranor, and R. W. Reeder. (2009). “A Published, sold and distributed by: nutrition label” for privacy”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.
- Kerner, S. (2022). “Colonial Pipeline hack explained: Everything you need to know”. URL: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>.
- Khan, B., K. S. Agrawal, and M. K. Khan. (2011). “Information security awareness campaign: An alternate approach”. In: *International Conference on Information Security and Assurance*. Springer.
- Kleinberg, P., Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, Tel. +1-617-633-1574, N. Gupta, and M. Reiter. (2012). “Tag, you can see it! Using tags for access control in photo sharing”. In: *Proceedings of the SIGCHI conference on human factors in computing systems*. S. Das et al.: The Security & Privacy Acceptance Framework (SPAF). Foundations and Trends in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.
- Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, B. Kantor, D. Anderson, H. Shacham, et al. (2010). “Experimental security analysis of a modern automobile”. In: *2010 IEEE symposium on security and privacy*. IEEE. 447–462.
- Kraemer, S. and P. Carayon. (2007). “Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists”. *Applied ergonomics*, 38(2): 143–154.
- Kroll, D. and S. Stieglitz. (2021). “Digital nudging and privacy: improving decisions about self-disclosure on social networks”. *Behavior on the internet at: www.copyright.com*
- Kropczynski, J., R. Chaumy, Anafaky, M. A. Kater, A. F. Godfrey, D. Lipford, and J. J. Vysniwskyi. (2021). “Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving”. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2): 1–23.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers, Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service provided on the internet at: www.copyright.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, Inc, PO Box 1024, Hanover, MA 02339, USA. Tel. +1 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this material must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

- Foundations and Trends® in Privacy and Security, Vol. 1, No. 1, 2022. “To Self-Persuade or be Persuaded: Examining Interventions for Users’ Privacy Setting Selection”. In: *CHI Conference on Human Factors in Computing Systems*. 1–17.
- Kumaraguru, P. and L. F. Cranor. (2005). *Privacy indexes: a survey of Published, sold and distributed by: Westin’s studies*. Carnegie Mellon University, School of Computer Science, Institute for ...
- Kumaraguru, P., J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. United States Blair, and T. Pham. (2009). “School of phish: a real-world evaluation of anti-phishing training”. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.
- Kumaraguru, P., S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. (2008). Lessons from a real world evaluation of anti-phishing training. In: *2008 eCrime Researchers Summit*. IEEE. 1–12.
- van der Vlist, S. (2013). “Making sense from Snowden: What’s significant in the NSA surveillance revelations”. *IEEE Security & Privacy*, 11(4): 54–63.
- The preferred citation for this publication is Lebeck, K., K. Ruth, T. Kohno, and F. Roesner. (2018). “Towards Foundational Privacy for multi-user augmented reality Foundations with end users”. In: *2018 IEEE Symposium on Security and Privacy*. ISBN: 978-1-4661-3825-1. © 2018 IEEE. 392–408.
- Lebek, B., J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler. (2013). “Employees’ information security awareness and behavior: A literature review”. In: *2013 46th Hawaii International Conference on System Sciences*. IEEE. 2978–2987.
- Lerner, A., F. Zeng, and F. Roesner. (2017). “Confidante: Usable encrypted email: A case study with lawyers and journalists”. In: *2017 IEEE European Symposium on Security and Privacy (EuroSecP)*. IEEE. 385–400.
- Li, I., E. B. Neundorfer, Y. Agarwal, and J. I. Hong. (2021). “Honey-suckle: Annotation-guided code generation of in-app privacy notices”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 5(3): 1–27. Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

- Y. C. T. and Y. C. T. (2017). “Privacystreams: Enabling transparency in personal data processing for mobile apps”. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 1(3): 1–26.
 Published, sold and distributed by:
 Licklider, J. C. (1960). “Man-computer symbiosis”. *IRE transactions on human factors in electronics*. (1): 4–11.
- H. H. and M. E. Zurko. (2012). “Someone to watch over me”. In: *Proceedings of the 2012 New Security Paradigms Workshop*. 67–76. Tel. +1-781-983-4510
 www.nowpublishers.com
- L. P., M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. S. Das, and A. Acquisti. (2016a). “Follow my recommendations: A personalized privacy assistant for mobile app users”. In: *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 27–41.
- L. P., G. Gao, K. Zhang, W. Gao, J. Liang, and L. Yang. (2016b). “When privacy meets usability: Unobtrusive privacy permission recommendation system for mobile apps based on crowdsourcing”. *IEEE Transactions on Services Computing*. 11(5): 864–878.
- S. Das et al.: *The Security & Privacy Acceptance Framework (SPAFA)*. Foundations and Trends in Privacy and Security, vol. 1, no. 1, pp. 2012, 2012. ISBN: 978-1-63328-119-1
- © 2012 De Gruyter
 “Personalized Privacy Overlays”. *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW1): 1–28.
- Ma, Y., J. Feng, L. Kumin, and J. Lazar. (2013). “Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users”. *ACM Transactions on Accessible Computing (TACAS)*. 4(1): 27.
- Malhotra, N. K., S. S. Kim, and J. Agarwal. (2004). “Internet users’ information privacy concerns (IUPC): The construct, its scale, and a causal model”. *Information systems research*. 15(4): 336–358.
 The copyright for this article is held by the copyright owner. For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com
- Mantylarvi, J., M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. Isoaho. (2005). “Identifying users of portable devices from gait pattern with accelerometer”. In: *Proceedings of ICASSP 05. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005*. Vol. 2. IEEE. ii–973.
 now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities.” In: *SOUPS*.

Maxwell, G. (2013). “CoinJoin: Bitcoin privacy for the real world”. In: *Post on Bitcoin forum*. Vol. 3. 110.

Published, sold and distributed by:
now Publishers Inc.

Mayer, P., H. Berket, and M. Volkamer. (2016). “Enabling automatic password change in password managers through crowdsourcing”.

Proc. AAAI WORDS. Springer.

Mazurek, M. L., P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor. (2011). “Exploring reactive access control”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

United States

Outside North America:

Myrre, F. L.; Y. Liang, W. Melicher, M. Sleeper, L. Bauer, G. R. Ganger, N. Gupta, and M. K. Reiter. (2014). “Toward strong, usable access control for shared distributed data”. In: *12th USENIX Conference on File and Storage Technologies (FAST 14)*. 89–103.

McCarthy, D.; D. Barua, J. Clark, S. Chiasson, and P. C. Van Oorschot. (2012). “Tapas: design, implementation and usability evaluation of a password manager”. In: *Proceedings of the 28th Annual Computer Security Applications Conference*. 89–98.

S. Das et al.. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Privacy and Security, vol. 13, no. 1, pp. 1–33, 2012. ISBN: 978-1-63329-119-1

McDonald, C., C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles. (2021). “It’s stressful having all these phones”: Investigating Sex Workers’ Safety Goals, Risks, and Practices Online”. In: *30th USENIX Security Symposium (USENIX Security 21)*.

McSweeney, T. (2018). “Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?” *Georg. Eng. Tech. Rev.* 2: 514–514.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorizations to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc. for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service provided that the fee of \$12.00 is paid directly to CCC. For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

Mandel, D., D. Gao, D. Lo, and E. Toon. (2021). “An Exploratory Study of Social Support Systems to Help Older Adults in Managing Mobile Safety”. In: *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. 1–14.

Mendel, N., S. Schuster, E. Froler, and E. Toon. (2022). “Toward Proactive Support for Older Adults: Predicting the Right Moment for Providing Mobile Safety Help”. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 16 (1): 1–14.

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use in print and electronic forms must be obtained from the publisher. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers, P.O. Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; sales@nowpublishers.com

Foundations and Trends in Privacy and Security

- Flaherty, M., J. L. Gill, and M. P. H. Smith. (2011). “Saying me! an empirical investigation of the usability of app privacy notifications”. In: *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. 371–375.
- Milka, G. (2018). “The Anatomy of Account Take-Over”. In: *USENIX Security*. URL: https://www.usenix.org/sites/default/files/protected-files/enigma18_milka.pdf.
- Moyet, M., H. Abdi, A. Lu, and S. Das. (2022). ““how do you not lose friends?”: Synthesizing a design space of social controls for securing shared digital resources via participatory design jams,” in: *Proceedings of the 31st USENIX Security Symposium (SEC)*.
- Mousser, F. and A. Rubin. (1997). “Authentication via keystroke dynamics”. In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. 48–56.
- McIntyre, J. and D. Roberts. (2013). “AP Twitter hack causes panic on Wall Street and sends Dow plunging”. URL: <http://www.theguardian.com/business/2013/apr/03/ap-tweet-hack-wall-street-freefall>.
- Mostafa, M. and O. S. Faragallah. (2019). “Development of serious games for teaching information security courses”. *IEEE Access*. 7: 16923–16935.
- Nag, S., K. S. Bhat, S. Das, and N. Kumar. (2021). “Individually vulnerable, collectively safe: The security and privacy practices of households with older adults”. *Proceedings of the ACM on Human-Computer Interaction*. 5(CSCW1): 1–24.
- Napoli, D., S. N. Chaparro, S. Chiasson, and E. Stobert. (2020). “Something Doesn’t Feel Right: Using Thermal Warnings to Improve User Security Awareness”. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–11.
- Ng, W. (2012). “Can we teach digital natives digital literacy?” *Computers & Education*. 99: 106–110.
- Nicholson, J., L. Coventry, and P. Briggs. (2019). ““ If It’s Important It Will Be A Headline Cybersecurity Information Seeking in Older Adults”. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

- Foundations and Trends in Privacy and Security** (2018). “Simple nudges for better password creation”. In: *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*. 1–12.
- Nielsen, J. and J. Alertbox. (2004). “User education is not the answer to security problems”. *Alertbox, October*.
Published, sold and distributed by:
 now Publishers Inc.
 Number 4, A. D. R. Horne, and D. A. Horne. (2007). “The privacy
 Hangar, MA 01838
 United States
 Tel. +1-781-985-4510
 www.nowpublishers.com
 sales@nowpublishers.com
- Norman, D. (2013). *The design of everyday things: Revised and expanded edition*. Basic books.
- Olthauson, M. K. (2014). “Privacy challenges and opportunities: The Federal Trade Commission”. *Journal of Public Policy & Marketing*. 33(1): 4–9.
now Publishers Inc.
 PO Box 179
 2600 AD Delft
 The Netherlands
 Tel. +31-71-749-1774
 www.nowpublishers.com
 sales@nowpublishers.com
- Olthauson, M. K. and A. Kanaoka. (2015). “Password strength meters using social influence”. In: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS’15)*. Usenix, Berkely, CA.
- Olmstead, K. and A. Smith. (2017). “Americans and Cybersecurity”. S. Das et al. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Privacy and Security, vol. 5, pp. 1–22. <https://www.nowpublishers.com/article/doi/10.1561/3300000026>
 ISBN: 978-1-65828-119-1
- Olthauson, M. K., A. Krauss, and B. Ur. (2021). “User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators”. In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 57–76.
- Park, C. Y., C. Faklaris, S. Zhao, A. Sciuto, L. Dabbish, and J. Hong. (2018). “Share and share alike: An exploration of secure behaviors in romantic relationships”. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 83–102.
now Publishers Inc.
 PO Box 179
 2600 AD Delft
 The Netherlands
 Tel. +31-71-749-1774
 www.nowpublishers.com
 sales@nowpublishers.com
- Parsons, K. D., Galic, M., Pattinson, M., Butavicius, A., Mcormac, and I. Zwaans. (2017). “The human aspects of information security questionnaires (HAIQ): two further validation studies”. *Computers & Security*. 66: 10–31.
now Publishers Inc.
 PO Box 179
 2600 AD Delft
 The Netherlands
 Tel. +31-71-749-1774
 www.nowpublishers.com
 sales@nowpublishers.com
- Pearman, S. S., A. Zhang, L. Bauer, N. Christin, and L. F. Cranor. (2019). “Why people (don’t) use password managers effectively”. In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 309–328.
now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this material for teaching and research purposes is granted by now Publishers Inc. for users registered with the Copyright Clearance Center (CCC). The services of users can be found on the internet at: www.copyright.com

Foundations and Trends in Privacy and Security

- Zhou, J., and Y. Zou. (2019). “Do you know where your link is: Improving and evaluating email phishing warnings”. In: *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–15.
- Rader, E., R. Wash, and B. Brooks. (2012). “Stories as informal lessons about security”. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.
- Redmiles, E. M. (2018). “Net benefits: Digital inequities in social capital, privacy preservation, and digital parenting practices of US social media users”. In: *Proceedings of the International AAAI Conference on Web and Social Media*. Vol. 12. No. 1.
- Redmiles, E. M., S. Kross, and M. L. Mazurek. (2016a). “How i learned to say no: A census-representative survey of security advice sources and behavior”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 666–677.
- Redmiles, E. M., S. Kross, and M. L. Mazurek. (2017). “Where is the digital divide? A survey of security, privacy, and socioeconomics”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.
- S. Das et al.: The Security & Privacy Acceptance Framework (SPAF). Foundations and Trends in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.
- Redmiles, E. M., A. R. Malone, and M. L. Mazurek. (2016b). “I think they’re trying to tell me something: Advice sources and selection for digital security”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. 272–288.
- Redmiles, E. M., M. L. Mazurek, and J. P. Dickerson. (2018). “Dancing pigs or externalities? Measuring the rationality of security decisions”. In: *Proceedings of the 2018 ACM Conference on Economics and Computation*. 215–232.
- Reeder, R. W., L. Bauer, L. F. Cranor, M. K. Reiter, and K. Bacon. (2011). “More than just a risk: Measuring effects of the underlying model on access-control system usability”. In: *Proceedings of the 2011 Conference on Human Factors in Computing Systems*. 2069–2074.
- Reeder, R. W., L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. (2008). “Expandable grids for visualizing and authoring computer security policies”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1473–1482.

Foundations and Trends® in Privacy and Security

- 141 D. D. M. T. S. P. W. P. and K. H. H. (2015). “Financial Exploitation of the Elderly in a Consumer Context”.
- Rezgui, Y. and A. Marks. (2008). “Information security awareness in higher education: An exploratory study”. *Computers & security*. 27(7-8): 241–253.
- Published, sold and distributed by:
 now Publishers Inc. Garcia, and J. J. De La Vega. (2009). “The importance of perceived trust, security and privacy in online trading systems”. *Information Management & Computer Security*. United States
 Tel. +1-781-985-4510
www.nowpublishers.com
- Roepke, R. and U. Schroeder. (2019). “The Problem with Teaching Defences against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education.” *CSEDU (2)*: 58–66.
- Rogers, E. M. (1962). *Diffusion of innovations*. Free Press of Glencoe. PO Box 179, 2600 AD Delft, The Netherlands
 Tel. +31-6-7145274
- Ruoti, S., J. Andersen, T. Hundertshagen, D. Zappala, and K. Seamons. (2016). “Private Webmail 2.0: Simple and easy-to-use secure email”. S. Das et al., *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Security and Privacy, *Annual Symposium on Usable Security and Technology*. 461–472. ISBN: 978-1-63825-149-1
- Ruoti, S., J. Andersen, D. Zappala, and K. Seamons. (2015). “Why Johnny still, still can’t encrypt: Evaluating the usability of a modern PGP client”. *arXiv preprint arXiv:1510.08555*.
- Ruoti, S. and K. Seamons. (2019). “Johnny’s journey toward usable secure email”. *IEEE Security & Privacy*. 17(6): 72–76.
- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.
- Rao, (2009). “Understanding and capturing people’s privacy policies on a mobile social networking application”. *Personal and ubiquitous computing*. 13(6): 401–412. Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com
- Sasse, M. (2003). “Computer security: Anatomy of a Usability Disaster, For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., P.O. Box 179, 2600 AD Delft, The Netherlands. Tel: +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Schaub, F., R. Balebako, A. L. Durity, and L. F. Cranor. (2015). “A design space for effective privacy notices”. In: *Eleventh symposium on usable security and privacy (SOUPS 2015)*. 1–17.

Foundations and Trends® in Privacy and Security

- Shay, D., S. E. Eneman, and W. R. Rouseff. (2000). “Size matters: what you know, but who you know: a social approach to last-resort authentication”. In: *Proceedings of the sigchi conference on human factors in computing systems*. 1983–1992.
- Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. Published, sold, and distributed by: John Wiley & Sons, now Publishers Inc.
- Scrago, J.-M. and J. Ophoff. (2019). “Lessons learned from an organizational information security awareness campaign”. In: *IFIP World Conference on Information Security Education*. Springer. 129–143. www.nowpublishers.com
- Siles, S., D. Weng, J. Zhang, H. Li, H. Zheng, and B. Y. Zhao. (2020). “Towards Protecting Privacy against Unauthorized Deep Learning Models”. In: *Proc. of the 29th USENIX Security Symposium*. PO Box 179, 2600 AD Delft, The Netherlands.
- Shay, D., L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. H. Mazurek, W. Melicher, S. M. Segreti, and B. Ur. (2015). “A spoonful of sugar? The impact of guidance and feedback on the password creation behavior”. In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2903–2912.
- S. Das et al.: The Security & Privacy Acceptance Framework (SPAF). Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022. ISBN: 978-1-65823-199-1
- Sheng, S., J. Broderick, C. A. Koranda, and J. J. Hyland. (2006). “Why Johnny still can’t encrypt: evaluating the usability of email encryption software”. In: *Symposium On Usable Privacy and Security*. ACM. 3–4.
- Sheng, S., B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. (2007). “Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phishing”. In: *Proceedings of the 3rd symposium on Usable privacy and security*. Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service at the internet at: www.copyright.com
- Shneiderman, B. and P. Maes. (1997). “Direct manipulation vs. interface agents”. *interactions*. 4(6): 42–61.
- For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Smith, H. J., S. J. Milberg, and S. J. Burke. (1996). “Information privacy: Measuring individuals’ concerns about organizational practices”. *Information security awareness: Information management & computer security*. 167–196.

Foundations and Trends in Privacy and Security

- McAfee.
- Solove, D. J. (2007). "I've got nothing to hide and other misunderstandings of privacy". *San Diego L. Rev.* 44: 745.
- Song, Y., C. Faklaris, Z. Cai, J. I. Hong, and L. Dabbish. (2019). "Normal Published, sold and distributed by: and easy: Account sharing practices in the workplace". *Proceedings of the ACM on Human-Computer Interaction*. 3(CSCW): 1–25.
- Spiekermann, S. (2007). "Perceived control: Scales for privacy in ubiquitous computing". In: *Digital Privacy*. Auerbach Publications. 289–304. Tel. +1-781-985-4510 www.nowpublishers.com
- Stanton, J., P. Mastaglio, K. Stam, and J. Jolton. (2004). "Behavioral Information Security: Two End User Survey Studies of Outsider Normal Information Security and Security Practices." *AMCIS*. (August): 2–8. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.2938&rep=rep1&type=pdf>.
- Stobert, E. and R. Biddle. (2014). "A password manager that doesn't remember passwords". In: *Proceedings of the 2014 New Security Paradigms Workshop*. 39–52.
- S. Das et al.: The Security & Privacy Acceptance Framework (SPAF). Foundations and Trends in Privacy and Security, vol. 12, no. 1, pp. 1–19, 2017. ISBN: 978-1-65825-119-1
- © 2022. *International Conference on Security and Privacy in Communication Systems*. Springer. 446–466.
- Story, P., D. Smullen, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. (2020). "From intent to action: Nudging users towards secure mobile payments". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 379–415.
- Strand, K. L. (2018). "Influencing factors and effectiveness of a security awareness campaign". *Master's Thesis*. NTNU.
- Stylidis, I., C. O. Thanos, A. Anagnostakis, and E. Zaitseva. (2016). "A review of continuous authentication using behavioral biometrics". In: *Proceedings of the South East European Design Automation Conference, Computer Networks and Social Media Conference*. 72–79.
- Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

Feldman, A., D. P. Brumley, and M. Cavallaro. (2014). “A primer of behavioral biometrics: motivation, current developments, and future trends”. In: *2014 International Conference on Cyberworlds*. IEEE. 271–278.

Sunshine, J., S. Egelman, H. Almuhiemedi, N. Atri, and L. F. Cranor. (2009). “Crying wolf: An empirical study of ssl warning effectiveness.” In: *2009 USENIX security symposium*. Montreal, Canada. 399–416. Published, sold and distributed by: now Publishers Inc. PO Box 179, 2600 AD Delft, The Netherlands. Tel. +1-781-985-4510. www.nowpublishers.com

Thaler, R. H., and C. R. Sunstein. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin. Tel. +1-781-985-4510. www.nowpublishers.com

Thompson, J. E., MacRae, and A. Salehi-Abari. (2013). “Usability and security evaluation of GeoPass: a geographic location-password scheme”. In: *Proceedings of the Ninth symposium on usable privacy and security*. Now Publishers Inc. PO Box 179, 2600 AD Delft, The Netherlands. Tel. +1-781-985-4510. www.nowpublishers.com

Tiefenau, C., M. Häring, K. Krombholz, and E. Von Zezschwitz. (2020). “Security availability, and multiple information sources: Exploring the behavior of system administrators”. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 239–258. The Netherlands. Tel. +1-781-985-4510. www.nowpublishers.com

Tiefenau, C., E. von Zezschwitz, M. Häring, K. Krombholz, and M. Smids. (2019). “A usability evaluation of Let’s Encrypt and Certbot: usable security done right”. In: *Proceedings of the 2019 ACM Conference on Computer and Communications Security*. 1971–1988. © 2019 ACM. ISBN: 978-1-4503-5828-1

Ur, B., F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. F. Cranor, H. Dixon, P. Emami Naeini, H. Habib, et al. (2017). “Design and evaluation of a data-driven password meter”. In: *Proceedings of the 2017 ACM conference on human factors in computing systems*. 3775–3786.

Vance, A. B., B. Jenkins, B. B. Anderson, D. B. Bjornson, and C. B. Kiewan. (2018). “Timing out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments”. In: *The Quantitative User Experience*. 369–380.

Vance, A. B., B. Jenkins, D. Bjornson, and B. B. Anderson. (2017). “What do we really know about how habituation to warnings occurs over time? A longitudinal fMRI study of habituation and polymorphic warnings”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2215–2227.

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. The fee code for users of the Transactional Reporting Service is 0898-9290/2021 \$15.00. For all other use, permission should be sought from Cambridge University Press. This article is intended solely for the personal use of the individual user and is not to be disseminated broadly. © 2021 Cambridge University Press. This is a Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction in any medium, provided the original work is properly cited. This is a Creative Commons licensed article. For more information, see <http://www.cambridge.org/core/terms>. <https://doi.org/10.1017/S0898929021000026>

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Organizations in the USA who are also registered with the Copyright Clearance Center may therefore copy material (beyond the limits permitted by sections 107 and 108 of US copyright law) subject to payment to CCC of the per copy fee of \$12.00. This consent does not extend to multiple copying for promotional or commercial purposes. ISI Tear Sheet Service, 3501 Market Street, Philadelphia, PA 19104, USA, is authorized to supply single copies of separate articles for private use only. Organizations authorized by the Copyright Licensing Agency may also copy material subject to the usual conditions. For all other use, permission should be sought from Cambridge or the American Branch of Cambridge University Press.

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. The fee code for users of the Transactional Reporting Service is 0898-9290/2021 \$15.00. For all other use, permission should be sought from Cambridge University Press. This article is intended solely for the personal use of the individual user and is not to be disseminated broadly. © 2021 Cambridge University Press. This is a Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction in any medium, provided the original work is properly cited. This is a Creative Commons licensed article. For more information, see <http://www.cambridge.org/core/terms>. <https://doi.org/10.1017/S0898929021000026>

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. The fee code for users of the Transactional Reporting Service is 0898-9290/2021 \$15.00. For all other use, permission should be sought from Cambridge University Press. This article is intended solely for the personal use of the individual user and is not to be disseminated broadly. © 2021 Cambridge University Press. This is a Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction in any medium, provided the original work is properly cited. This is a Creative Commons licensed article. For more information, see <http://www.cambridge.org/core/terms>. <https://doi.org/10.1017/S0898929021000026>

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. The fee code for users of the Transactional Reporting Service is 0898-9290/2021 \$15.00. For all other use, permission should be sought from Cambridge University Press. This article is intended solely for the personal use of the individual user and is not to be disseminated broadly. © 2021 Cambridge University Press. This is a Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution and reproduction in any medium, provided the original work is properly cited. This is a Creative Commons licensed article. For more information, see <http://www.cambridge.org/core/terms>. <https://doi.org/10.1017/S0898929021000026>

- Foundations and Trends in Privacy and Security** of sight, out of mind: Effects of displaying access-control information near the item it controls”. In: *2012 Tenth Annual International Conference on Privacy, Security and Trust*. IEEE. 128–136.
- Vanica, K. and Y. Rashidi. (2016). “Tales of software updates: The process of updating software”. In: *Proceedings of the 2016 chi conference on human factors in computing systems*. 3215–3226.
- Vanier, M. A., E. Rader, and R. Wash. (2014). “Betrayed by updates: how negative experiences affect future security”. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2671–2674.
- Vannini, S. R. Gomez, and B. C. Newell. (2020). ““Mind the five”: Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations”. *Journal of the Association for Information Science and Technology*. 71(8): 927–938.
- Venkatesh, V. and H. Bala. (2008). “Technology acceptance model 3 and a research agenda on interventions.” *Decision sciences*, 39(2): 273–285.
- S. Das et al., *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.
- Venkatesh, V. and F. D. Davis. (2000). “A theoretical extension of the Technology acceptance model: Four longitudinal field studies”. *Management science*. 46(2): 186–204.
- Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis. (2003). “User acceptance of information technology: Toward a unified view”. *MIS quarterly*: 425–478.
- Verizon (2020). “Data Breach Investigations Report”. *Tech. rep.*
- Verizon. (2022). “Data Breach Investigations Report”. *Tech. rep.*
- Wang, Y. C., B. K. Rana, and J. M. Lewone. (2012). “To stay or leave? The relationship of emotional and informational support to commitment in online health support groups”. In: *Proceedings of the ACM 2012 conference on computer supported cooperative work*. 833–842.
- Wang, Y. H., Jin, and N. Li. (2009). “Sensible access control in collaborative environments: Authorization based on people-tagging”. In: *European Symposium on Research in Computer Security*. Springer. 268–284.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) Transactional Reporting Service, provided that the fee of \$12.00 per copy is paid directly to CCC. For those organizations that have been granted a photocopy licence, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc, P.O. Box 1021, Hanover, MA 03330, USA. Tel. +1 871 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends in Privacy and Security

- Wang, J., Fokla, J., Palanisubramanian, J., and Hogg (2023). "It's Problematic but I'm not Concerned": University Perspectives on Account Sharing". *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW1): 1–27.
- Wang, Y. (2018). "Inclusive security and privacy". *IEEE Security & Privacy*, 16(4): 82–87.
- Wang, Y., P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. (2014). "A field trial of privacy nudges for facebook". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. Tel. +1-781-985-4510
www.nowpublishers.com
- Wasil, R. (2010). "Folk models of home computer security". In: *Proc. SOUPS '10*. New York, New York, USA: ACM Press. 1. DOI: 10.1145/1837125.
- Wassenaar, E., Rader, K., Vaniea, and M. Rizor. (2014). "Out of the box: How automated software updates cause unintended security consequences". In: *10th Symposium On Usable Privacy and Security (SOUPS:2014)*. 89–104.
- WebAIM (2017). "Screen Reader User Survey #7 Results". S. Das et al., *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends in Privacy and Security (2019) 5, no. 1, pp. 1–32. ISBN: 978-1-60382-119-1
- Whitten, A. and J. Tygar (1999) 5, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0". In: *Proc. SSYM'99*. 14–28. URL: http://www.usenix.org/events/sec99/full_papers/whitten/whitten.ps.
- Wickins, J. (2007). "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification". *Science and Engineering Ethics*. 13(1): 45–54.
- All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publishers.
- Wikipedia (2021). "2017 Equifax data breach". https://en.wikipedia.org/wiki/2017_Equifax_data_breach.
- Wilson, G. H., Maxwell, and M. Just (2017). "Everything's Cool, But Use of the Internal or Personal Use of Specific Clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC) The Feedback for users can be found on the internet at: www.copyright.com
- For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc, PO Box 1021, Hanover, MA 02331, USA. Tel: 871 0245; www.nowpublishers.com; sales@nowpublishers.com
- Wolcott, J. O. (2009). "applies tapping rhythm-based passwords on a single binary sensor". In: *Proceedings of the 22nd annual ACM symposium on User interface software and technology*. 93–96.
- Wolcott, J. O. (2006a). "Behavioral compliance: The research methodology, Publishers, PO Box, 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com
- and results in: *Handbook of warnings*. CRC Press. 335–354.

- Woo, S., E. Kaiser, R. Artstein, and J. Mirkovic. (2016). “Life-experience passwords (leps)”. *Handbook of warnings*: 51–61.
- Woo, S., E. Kaiser, R. Artstein, and J. Mirkovic. (2016). “Life-experience passwords (leps)”. In: *Proceedings of the 32nd Annual Conference on Computer Security Applications*. 113–126.
- Wu, Y., W. K. Edwards, and S. Das. (2022a). ““A Reasonable Thing to Ask For”: Towards a Unified Voice in Privacy Collective Action”. In: *CHI Conference on Human Factors in Computing Systems*. 1–17.
- Wu, Y., W. K. Edwards, and S. Das. (2022b). “SoK: Social Cyber-security”. In: *IEEE Symposium on Security and Privacy (Oakland)*. <https://sawvikdas.com/uploads/paper/pdf/36/file.pdf>.
- Xiao, S., J. Witschey, and E. Murphy-Hill. (2014). “Social influences on development tool adoption: why security tools spread”. In: *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. 1095–1106.
- Xu, H., S. Ghosh, M. B. Rosson, and J. M. Carroll. (2012). “Measuring mobile users’ concerns for information privacy”. *The mobile user’s concerns for information privacy*.
- Yao, Y., D. Lo, R. and Y. Wang. (2017). “Folk models of online behavior: a study on advertising”. In: *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ISBN: 978-1-4503-1191-9.
- Yildirim, M. and I. Mackie. (2019). “Encouraging users to improve password security and memorability”. *International Journal of Information Security*. 18(6): 741–759.
- Zhang, Z., Z. Zhang, H. Yuan, N. M. Barbosa, S. Das, and Y. Wang. (2021). “Web Ally: Making Visual Task-based CAPTCHAs Transferable for People with Visual Impairments”. In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 284–298.
- Zhao, H., Y. and C. Henderson. (2014). “Privacy-aware location privacy preference recommendations”. In: *Proceedings of the 11th international conference on mobile and ubiquitous systems: Computing, networking and services*. 120–129.
- Zuboff, S. (2019). “Big other: surveillance capitalism and the prospects of an information civilization”. *Journal of information technology*. 30(1): 75–89.

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. See www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this material must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends® in Privacy and Security In:
Proceedings of the 1996 workshop on New security paradigms. 27–33.

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

ISBN: 978-1-63828-119-1

© 2022 S. Das *et al.*

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The ‘services’ for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com