Examining the Adoption and Abandonment of Security, Privacy and Identity Theft Protection Practices

Yixin Zou, Kevin Roundy,
Acar Tamersoy, Saurabh Shintre,
Johann Roturier, Florian Schaub

NortonLifeLock™

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

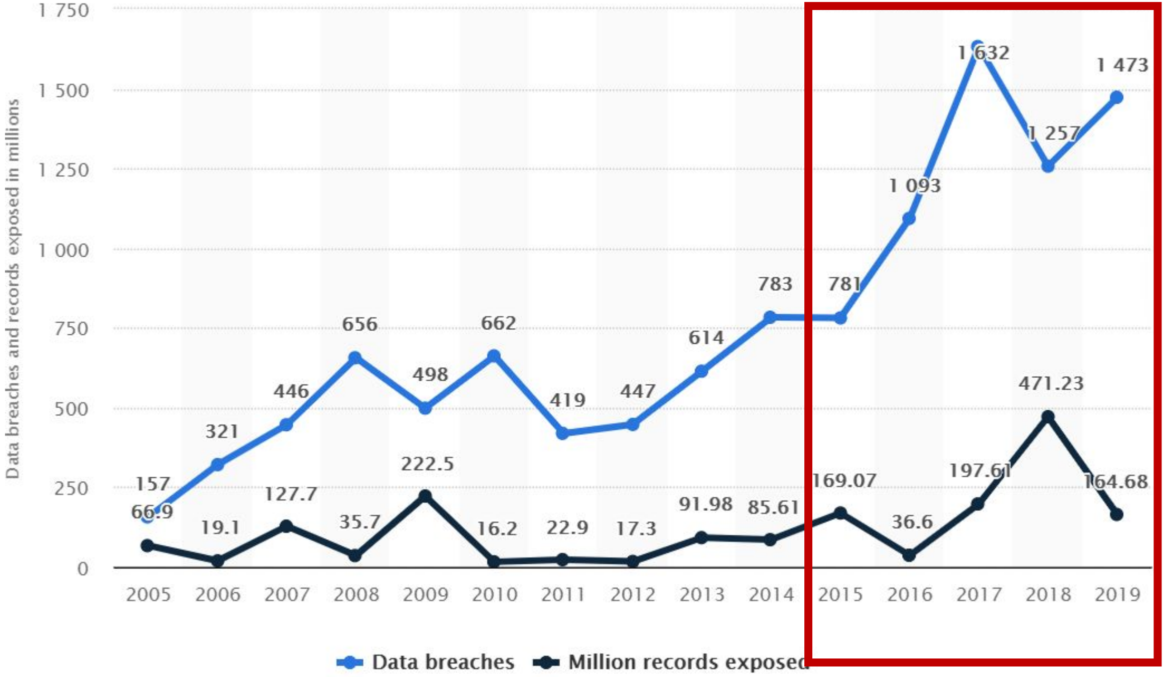
PRIVACYCON

The paper is published at CHI 2020 with a best paper honorable mention award.
This research is supposed by a NortonLifeLock Research Fellowship.

Consumers need to know how to protect their online safety

Lots of expert advice on online security and privacy self-protection

…but most consumers do not adopt best online security practices



PRIVACYCON

Source: Identity Theft Resource Center, Statista

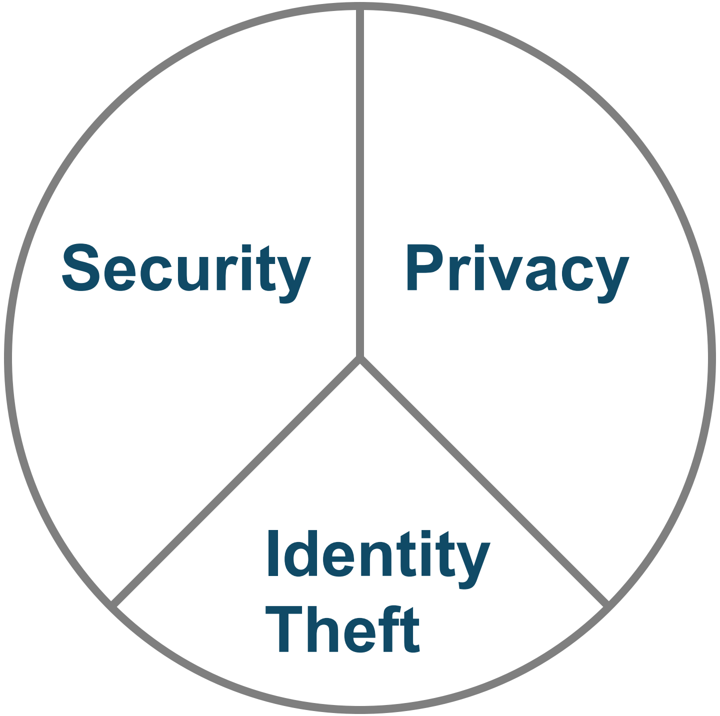
What we don’t know…

The adoption of other practices related to one’s online safety, such as those for **privacy** and **identity theft protection**.

What happens after the initial advice adoption, such as **how often and why consumers abandon advice after initial adoption**.

Research questions

1. **Which** practices are fully adopted, partially adopted, or abandoned?
2. **What** factors predict the level of adoption?
3. **Why** are certain practices partially adopted or abandoned?



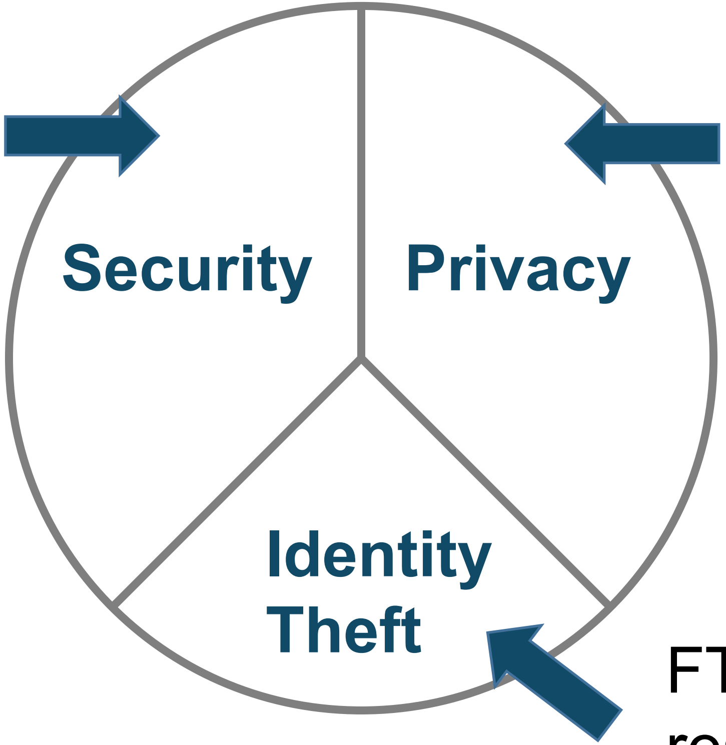
Security

Privacy

Identity Theft

Selected 30 expert-recommended practices

Ion et al.’s 2015 study, replicated by Busse et al., 2019. **(N=12)**



Security

Privacy

Identity Theft

A U.S. census representative 2015 Pew survey. **(N=12)**

FTC’s online resources. **(N=6)**

Security

- 2FA
- Antivirus
- Attachment clicking
- Link clicking
- Check URL
- Check HTTPS
- Automatic update
- Update software
- Install software
- Password manager
- Strong password
- Unique password

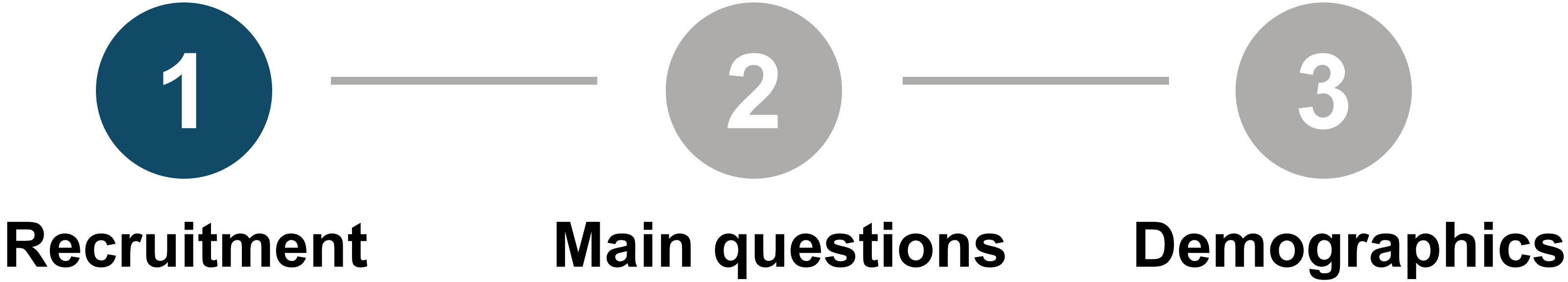
Privacy

- Anonymity system
- Encryption
- Private browsing
- Use public comp
- Browser extensions
- Clean cookies
- Disable cookies
- Hide info
- Avoid real name
- Use fake identities
- Search engine choice
- Facial recognition

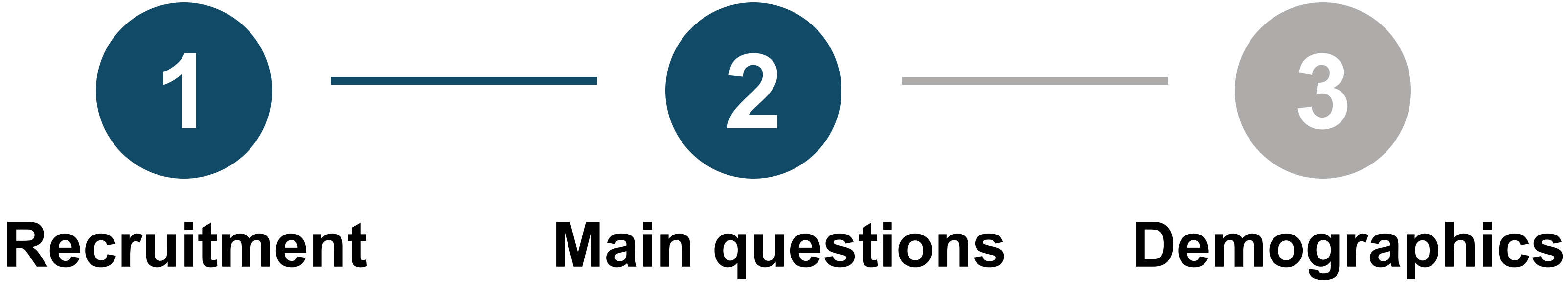
Identity

- Credit freeze
- Fraud alert
- Check credit reports
- Check statements
- Credit monitoring
- Identity monitoring

Note: the paper includes full text for each practice.



902 participants recruited via **Prolific**

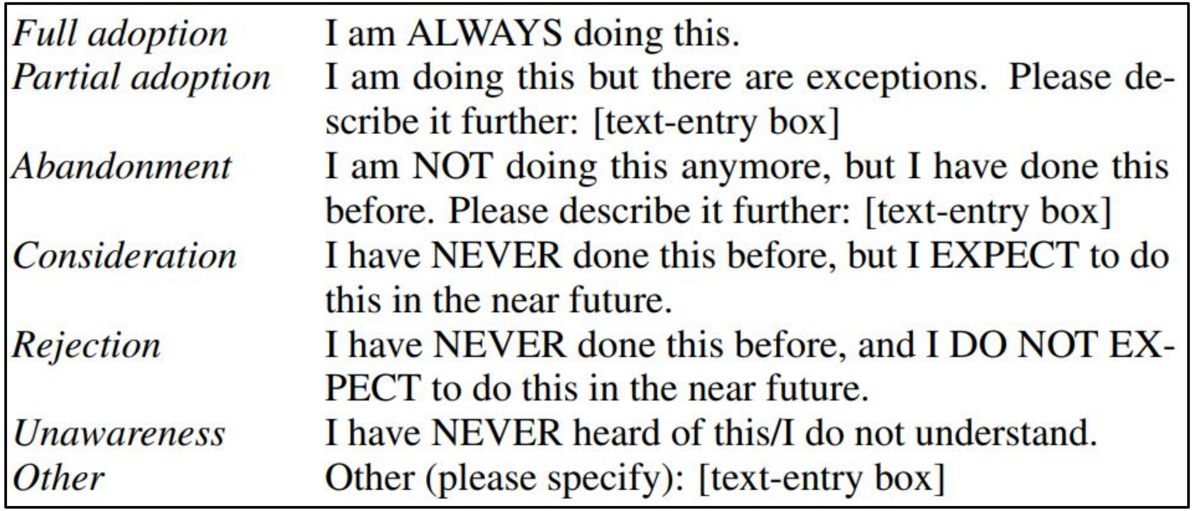


1 Recruitment

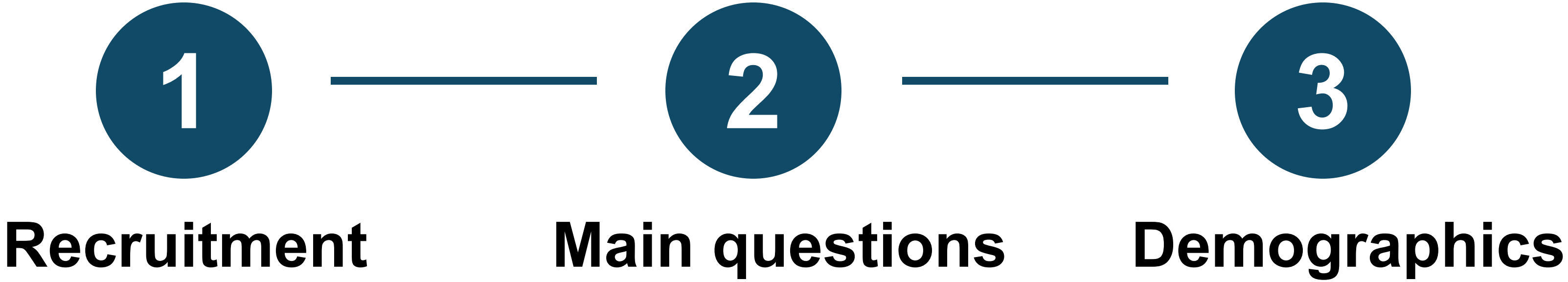
2 Main questions

3 Demographics

Display **10 practices** randomly selected from the list (~300 responses per practice).



Full adoption	I am ALWAYS doing this.
Partial adoption	I am doing this but there are exceptions. Please describe it further: [text-entry box]
Abandonment	I am NOT doing this anymore, but I have done this before. Please describe it further: [text-entry box]
Consideration	I have NEVER done this before, but I EXPECT to do this in the near future.
Rejection	I have NEVER done this before, and I DO NOT EXPECT to do this in the near future.
Unawareness	I have NEVER heard of this/I do not understand.
Other	Other (please specify): [text-entry box]



1 Recruitment

2 Main questions

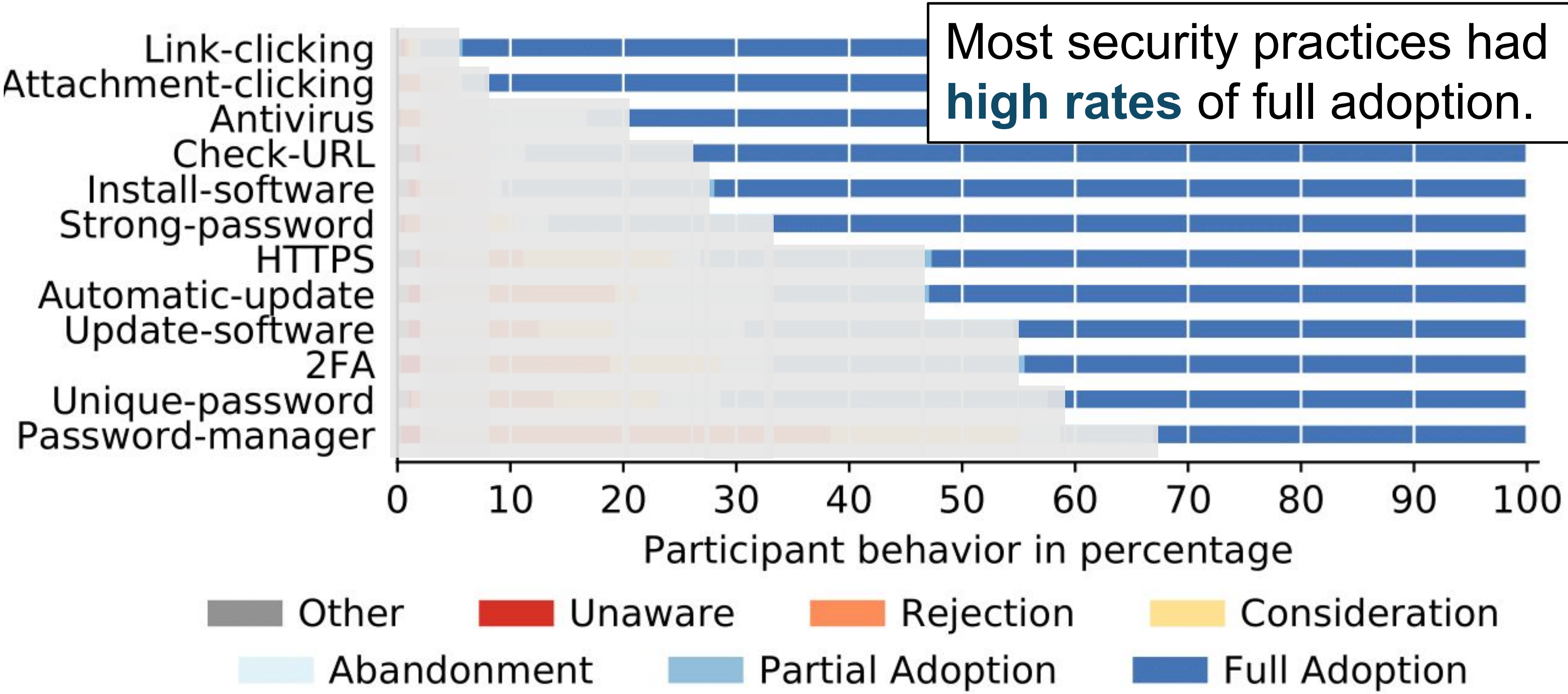
3 Demographics

- Gender and income distributions representative of U.S. population
- Younger and more educated compared to U.S. population

Key Findings:

Overview of practice adoption and abandonment

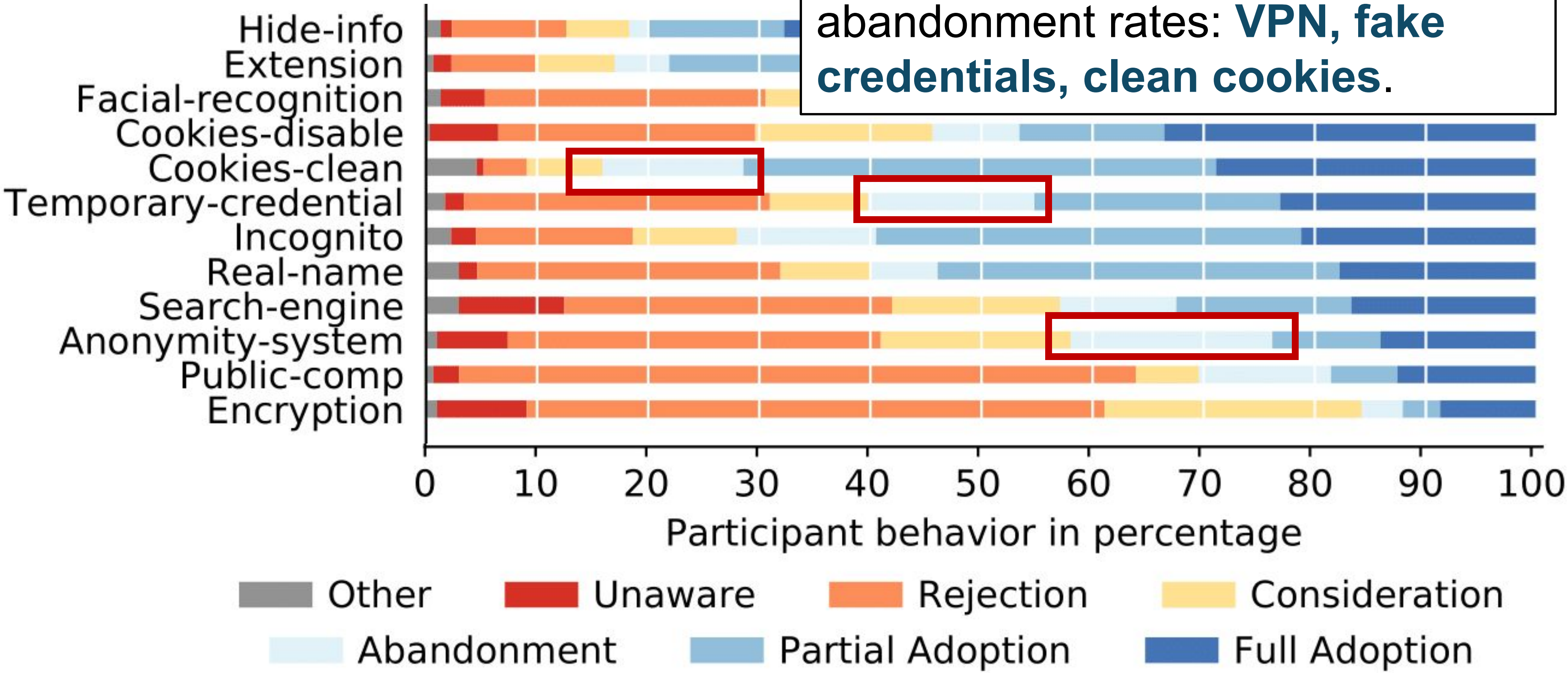
High adherence to security practices



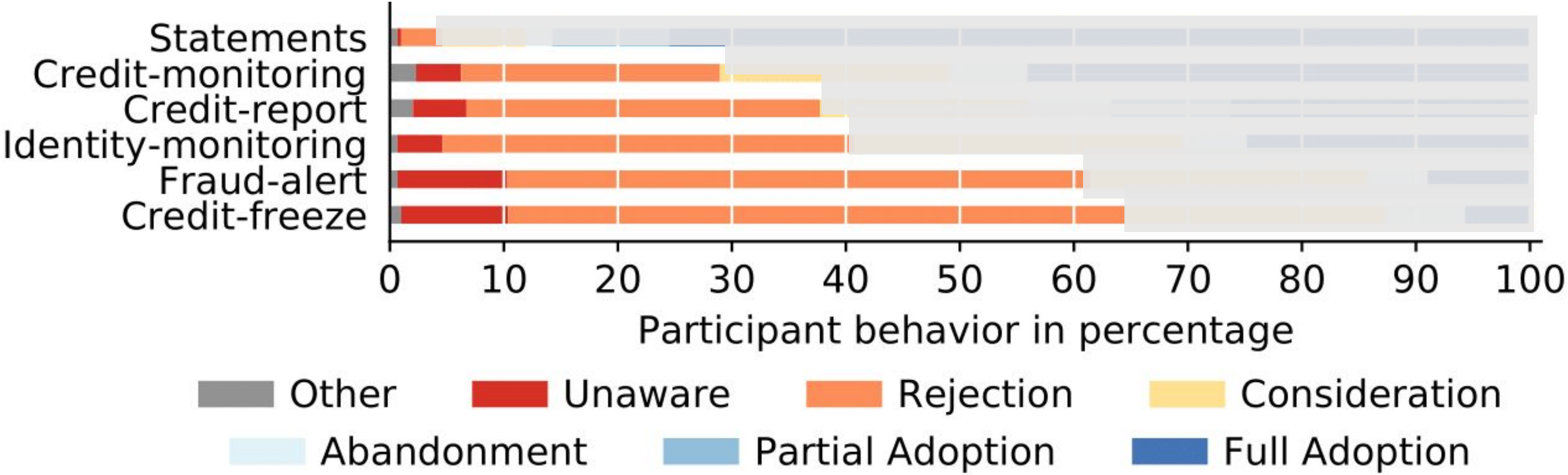
Most security practices had **high rates** of full adoption.

Most abandoned practices are privacy related

Practices with the highest abandonment rates: **VPN, fake credentials, clean cookies**.



Low adoption/acceptance of ID protections



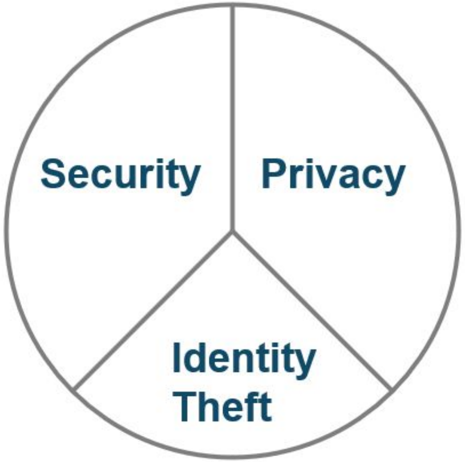
Participants were **unaware of or rejected** most ID protection practices, except checking financial statements

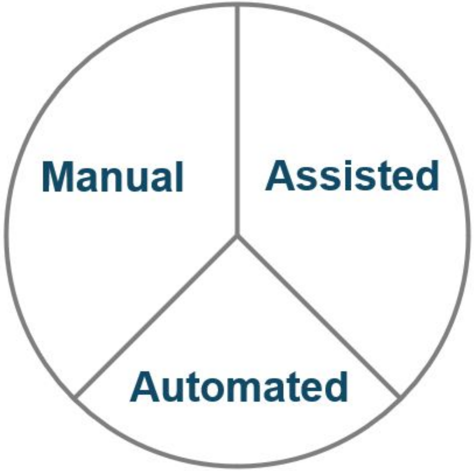
PRIVACYCON

Key Findings:

Factors affecting levels of adoption

Factors related to the practice





Area of practice

Security practices more adopted than privacy / anti identity theft practices.

Required user efforts

Assisted practices less adopted than manual / automated practices.

Factors related to the user

Technical background

Higher levels of adoption were correlated with expertise in computer science/IT more than security/privacy.

Prior negative experience

Being a victim of identity theft is a robust trigger for more practice adoption.

Key Findings:

Reasons behind partial adoption and abandonment

Common reasons for partial adoption

Only sensitive (11%)

> “I only did this for sensitive sites. [private browsing]”

Impracticality (10%)

> “If I’m in the middle of something I won’t do it.” [software update]

> “It’s hard to keep track. [unique passwords]”

Common reasons for abandonment

Not needed (20%)

> “I have used it but don’t find it all that helpful.” [private browsing]

Because of risk (14%)

> “I had a credit freeze due to suspected ID theft in 2012 when an unknown address in northern CA showed up on my credit report.” [credit freeze]

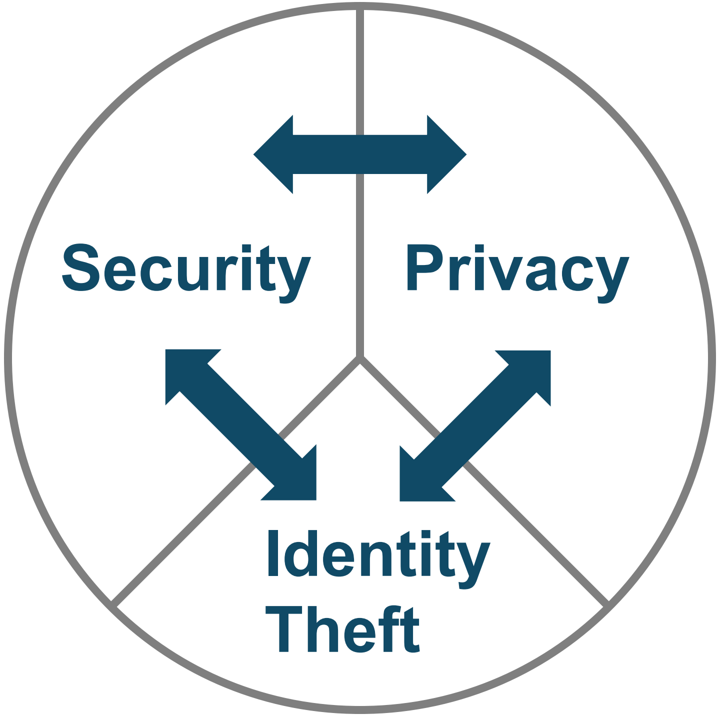
Recommendations:

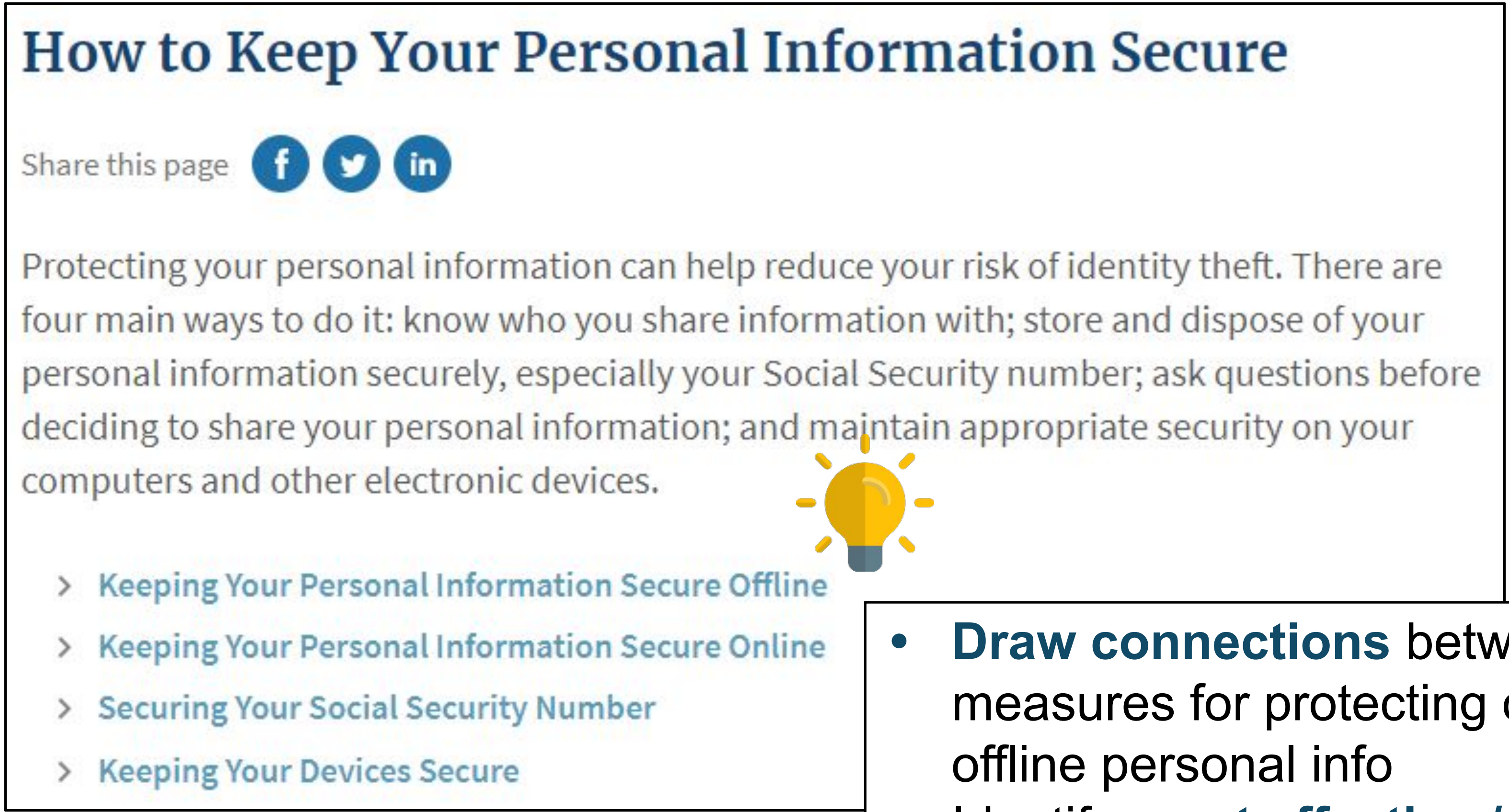
How to give expert advice

Bridge the gap between different areas of practices

E.g. to combat phishing scams, URL checking (security) and monitoring financial accounts (identity) are both needed.

Show the connections and benefits of **multi-layer approaches** in online safety protection.





How to Keep Your Personal Information Secure

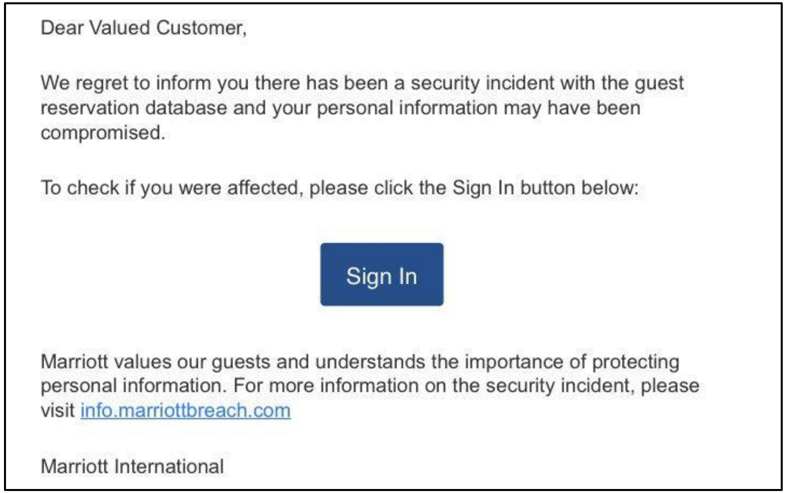
Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your Social Security number; ask questions before deciding to share your personal information; and maintain appropriate security on your computers and other electronic devices.

- Keeping Your Personal Information Secure Offline
- Keeping Your Personal Information Secure Online
- Securing Your Social Security Number
- Keeping Your Devices Secure

- **Draw connections** between measures for protecting online vs. offline personal info
- Identify **most effective / urgent actions** to be prioritized

Leverage at-risk situations for actionable consumer education

Data breaches as an example of at-risk situations


Dear Valued Customer,

We regret to inform you there has been a security incident with the guest reservation database and your personal information may have been compromised.

To check if you were affected, please click the Sign In button below:

Marriott values our guests and understands the importance of protecting personal information. For more information on the security incident, please visit info.marriottbreach.com

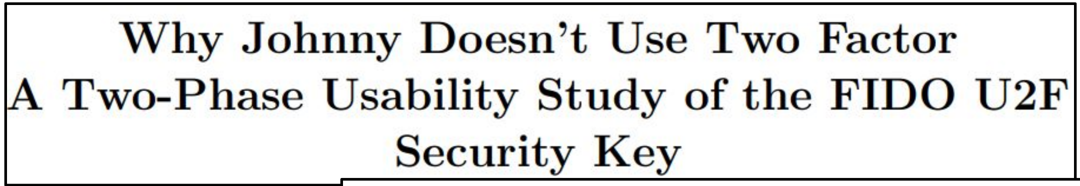
Marriott International

Consumer-facing breach notices as a possible venue for education

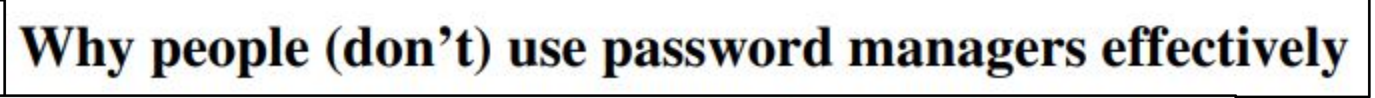
Recommendations:

Improve tools for online safety

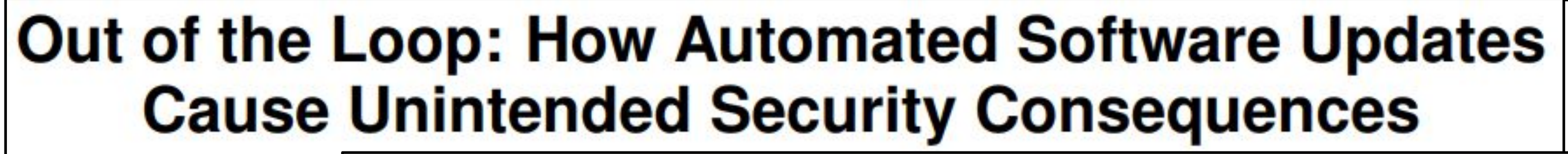
Usability issues prevent full adoption



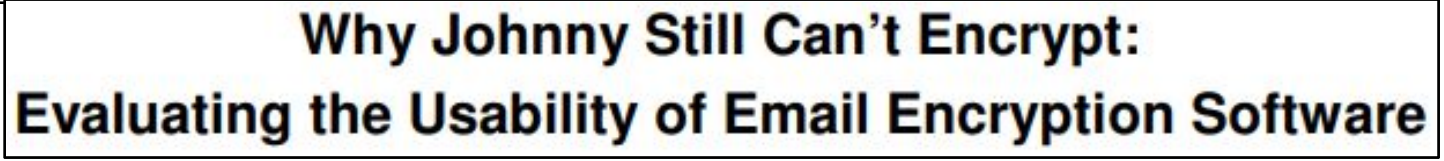
Why Johnny Doesn't Use Two Factor
A Two-Phase Usability Study of the FIDO U2F Security Key



Why people (don't) use password managers effectively



Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences



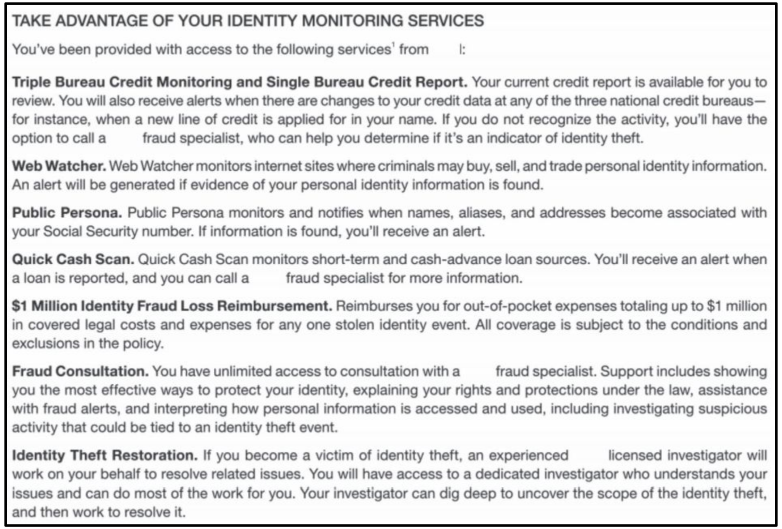
Why Johnny Still Can't Encrypt:
Evaluating the Usability of Email Encryption Software

Next steps for improving relevant tools

- More research to audit and solve usability issues of tools for **privacy / ID theft protection** (e.g., those for credit freezes and fraud alerts).

- **Require usability testing in regulations** to prevent companies from making mandated tools hard to use and reduce the burden on consumers.

Require usability testing in regulations



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from :

Triple Bureau Credit Monitoring and Single Bureau Credit Report. Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher. Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona. Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

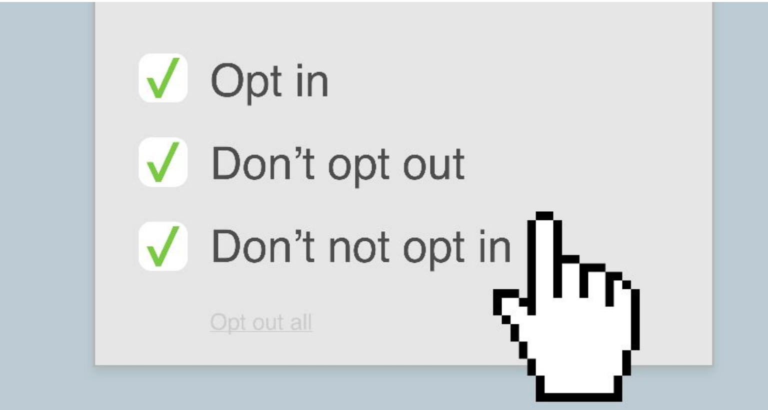
Quick Cash Scan. Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement. Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation. You have unlimited access to consultation with a fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Require **readability testing** of data breach notifications.



☑ Opt in

☑ Don't opt out

☑ Don't not opt in

Opt out all

Audit dark patterns in required privacy notices and controls.

Summary of take-aways

- Different patterns of adoption / abandonment for security vs. privacy vs. identity theft protection practices.
- Expert advice needs to bridge the gap between different areas of practices by emphasizing on their synergy effects.
- Tools for privacy and identity theft protection require more research to reduce user friction and encourage long-term adoption.

Contact: Yixin Zou (yixinz@umich.edu)