

Usable Security and Privacy Thinking & Threat Modeling

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

16/01/2024



THE UNIVERSITY
of EDINBURGH

Overview

- Warm-up discussion
- Fighting virus
- Threat modeling
- How to read and review a research paper?
- Take-home

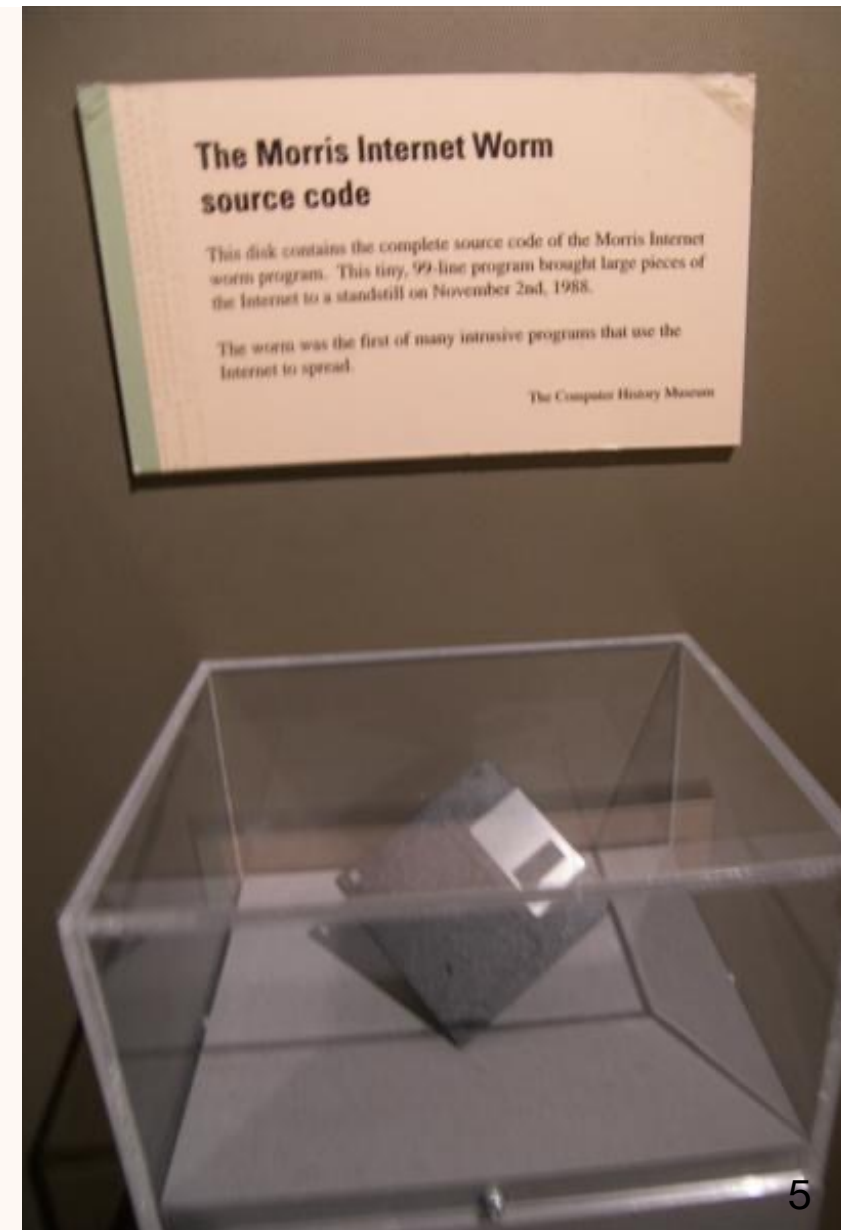
Discuss:

Do you know how safelink works? How do you feel about using it?

Problem: How do we keep bad software off from computers without upsetting users?

“Bad” software

- Worm
 - Self-propagating malicious software that “crawls” through the internet
 - Morris Internet Worm first example
 - Dangerous because no human involvement needed
- Virus
 - Malicious software that hides in other files and then infects the target.
 - Often viruses require some human interaction (click a link, plug in a USB, download a file)
- Potentially Unwanted Programs (PUP)
 - Full programs that provide functionality but the user may not actually want them.
 - Require some type of human interaction to install, but are often sneaky in how they explain themselves
 - Ask Toolbar



BILL GATES: TRUSTWORTHY COMPUTING

*This is the e-mail Bill Gates sent to every full-time employee at Microsoft, in which he describes the company's new strategy emphasizing security in its products. *From: Bill Gates

Sent: Tuesday, January 15, 2002 5:22 PM

To: Microsoft and Subsidiaries: All FTE

Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing - or able - to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

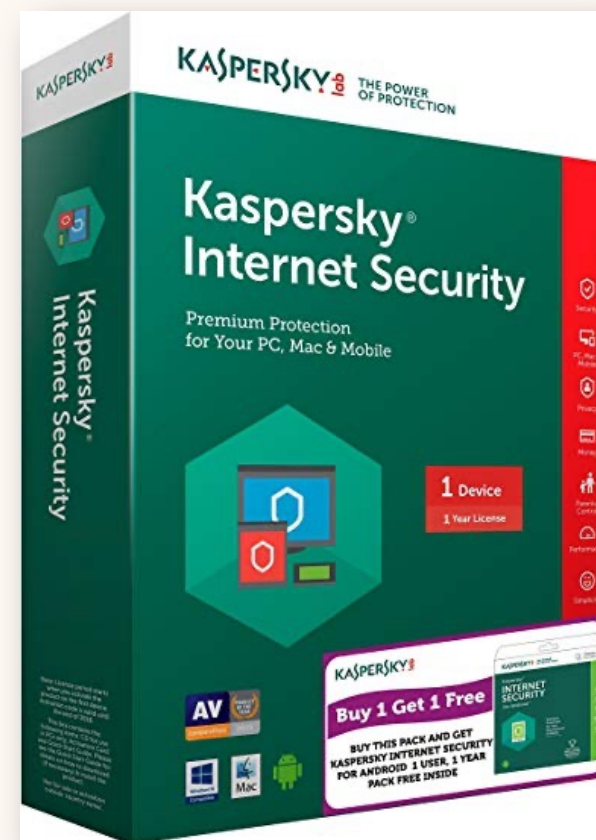
Still solving worms

- WannaCry and NotPetra were both worms released in 2017
- They targeted an open printer port, thereby avoiding the first defense of a firewall
- Open ports



Solving Viruses

- Antivirus tries to match known bad patterns against code on the computer
- Requires end user to spend money
- Can expire
- When expired keeps running, but no longer downloads lists of known bad code
- 2006 Windows Defender made freely available



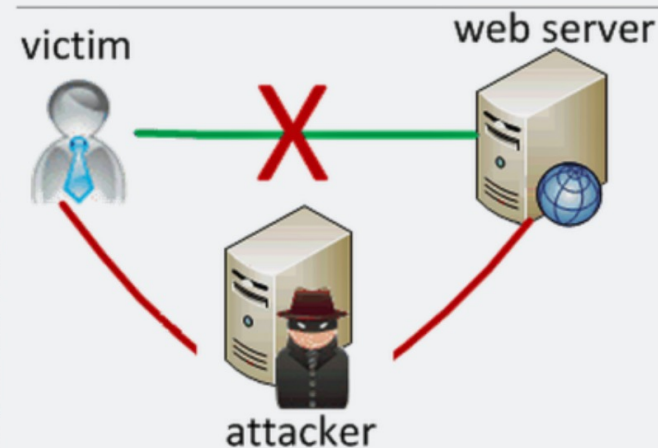
Potentially Unwanted Programs (PUPs)

- Do people really want things like copy protection and SuperFish?
- Should we auto-uninstall things that are not technically attacking?

Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - FEB 19, 2015 4:36 PM UTC



333



Lenovo is selling computers that come preinstalled with adware that hijacks encrypted Web sessions and may make users vulnerable to HTTPS man-in-the-middle attacks that are trivial for attackers to carry out, security researchers said.

The critical threat is present on Lenovo PCs that have adware from a company called Superfish installed. As unsavory as many people find software that injects ads into Web pages, there's something much more nefarious about the Superfish package. It installs a self-signed root HTTP certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

So...are we secure enough today?

Who are the “bad guys” and “good guys”

Adversaries

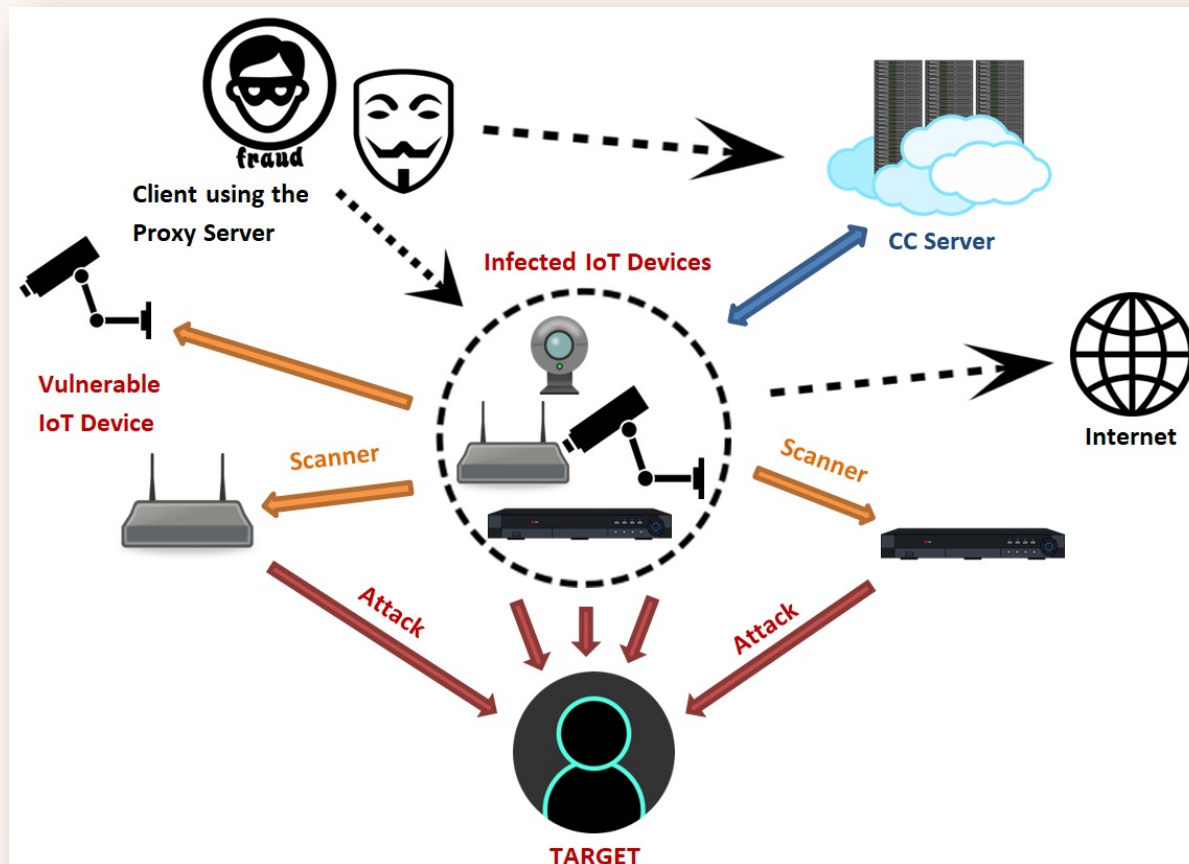
- Malicious actors
 - Hacker
 - Users (your family, your friend, your customer, etc.)
- Service providers
 - Company
 - App developers
- “Big brother”
- ... (depending on your position)

What are you protecting?

Assets

- Computer hardware: phone, laptop, server...
- Computer software: apps, operating systems, database...
- Physical assets: house, car.....
- Information: health record, your profile/identity, business info...
- Emotion, reputation, user experience....

Attack on IoT devices



<https://www.hackread.com/website-streams-from-private-security-cameras/>

- IoT devices can be overlooked and lacked proper protection/management

What can the bad guys do?

Risk, threat and vulnerability

- Vulnerability: the weakness of X (system/human) that can be exploited
 - The program is overprivileged to access things
 - The user reuses their password across applications
- Threat is an action performed by the adversary to damage the asset by exploiting a vulnerability
- Risk = asset X threat X vulnerability

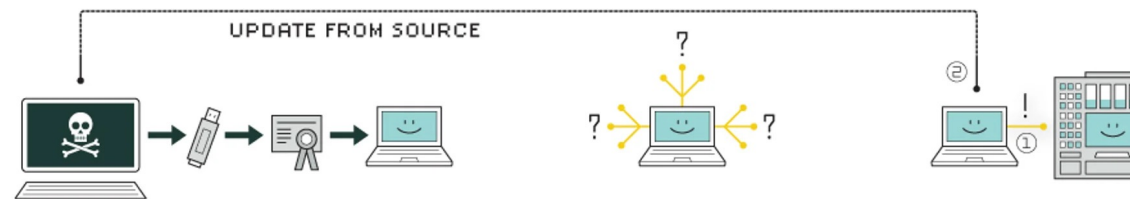
Stuxnet: a worm that targets nuclear facilities



- Jan 2010 – International Atomic Energy Agency found out a nuclear plant in Iran is malfunctioning
- Five months later, people confirmed that it is a result of an intended cyber attack. How?

Stuxnet: a worm that targets nuclear facilities

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Are we still falling behind?

You're not receiving security updates

Your version of Windows 10 has reached the end of service and isn't receiving security updates. These updates help protect your PC from viruses, spyware, and malware. To maintain the security of your device and data, we recommend you update to a newer version of Windows 10. Select 'Check for updates' for info on how to get this free update.

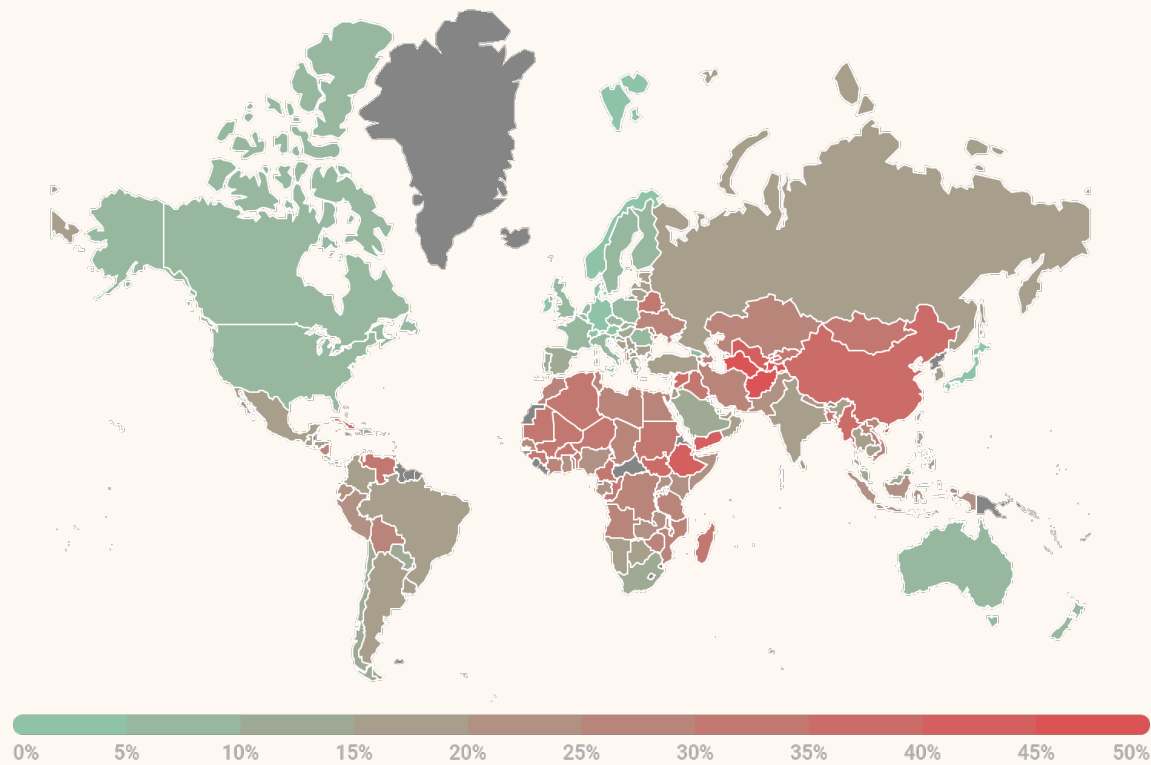
Don't show again

Remind me later


Check for updates

Lack of support/security update

Geographical difference of malware infection



- IoT devices can be overlooked and lacked proper protection/management

<https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/> 

Gap in security literacy and behavior

“...no one can hack my mind”: Comparing Expert and Non-Expert Security Practices

Iulia Ion
Google
iuliaion@google.com

Rob Reeder
Google
rreeder@google.com

Sunny Consolvo
Google
sconsolvo@google.com

ABSTRACT

The state of advice given to people today on how to stay safe online has plenty of room for improvement. Too many things are asked of them, which may be unrealistic, time consuming, or not really worth the effort. To improve the security advice, our community must find out what practices people use and what recommendations, if messaged well, are likely to bring the highest benefit while being realistic to ask of people. In this paper, we present the results of a study which aims to identify which practices people do that they consider most important at protecting their security online. We compare self-reported security practices of non-experts to those of security experts (i.e., participants who reported having five or more years of experience working in computer security). We report on the results of two online surveys—one with 231 security experts and one with 294 MTurk participants—on what the practices and attitudes of each group are. Our findings show a discrepancy between the security practices that experts and non-experts report taking. For instance, while experts most frequently report installing software updates, using two-factor authentication and using a password manager to stay safe online, non-experts report using antivirus software, visiting only known websites, and changing passwords frequently.

1. INTRODUCTION

Frightening stories about cybersecurity incidents abound. The

carefully considering the most worth-while advice to recommend is imperative. Even if users accept some responsibility for protecting their data [23, 43] and want to put in some effort [41], we should be thoughtful about what we ask them to do [20] and only offer advice that is effective and realistic to be followed.

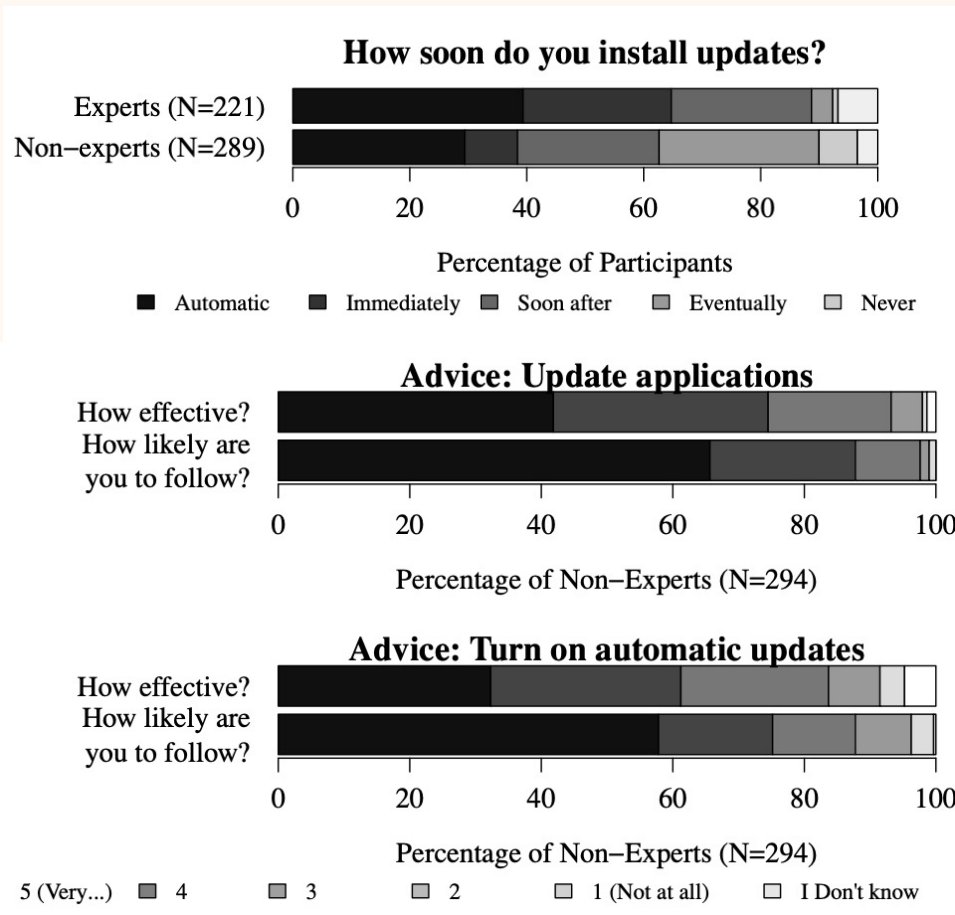
Existing literature on giving good advice suggests that for recipients to follow it, the advice should be (a) useful, comprehensible and relevant, (b) effective at addressing the problem, (c) likely to be accomplished by the recipient, and (d) not possess too many limitations and drawbacks [34]. Therefore, to improve the state of security advice, we must assess which actions are most likely to be effective at protecting users, understand what users are likely and willing to do, and identify the potential challenges or inconveniences caused by following the advice. Furthermore, lessons from health advice in outreach interventions suggest that people will not initiate certain actions if they do not believe them to be effective [53]. Therefore, to learn how to best deliver the advice to users, we must also understand how users perceive its effectiveness and limitations.

In preliminary work, we surveyed security experts to identify what advice they would give non-tech-savvy users. The most frequently given pieces of advice were, in order of frequency: (1) keep systems and software up-to-date, (2) use unique passwords, (3) use strong passwords, (4) use two-factor authentication, (5) use antivirus software, and (6) use a password manager. In this paper, we report on results of a study which tries to identify what security

Gap in security literacy and behavior

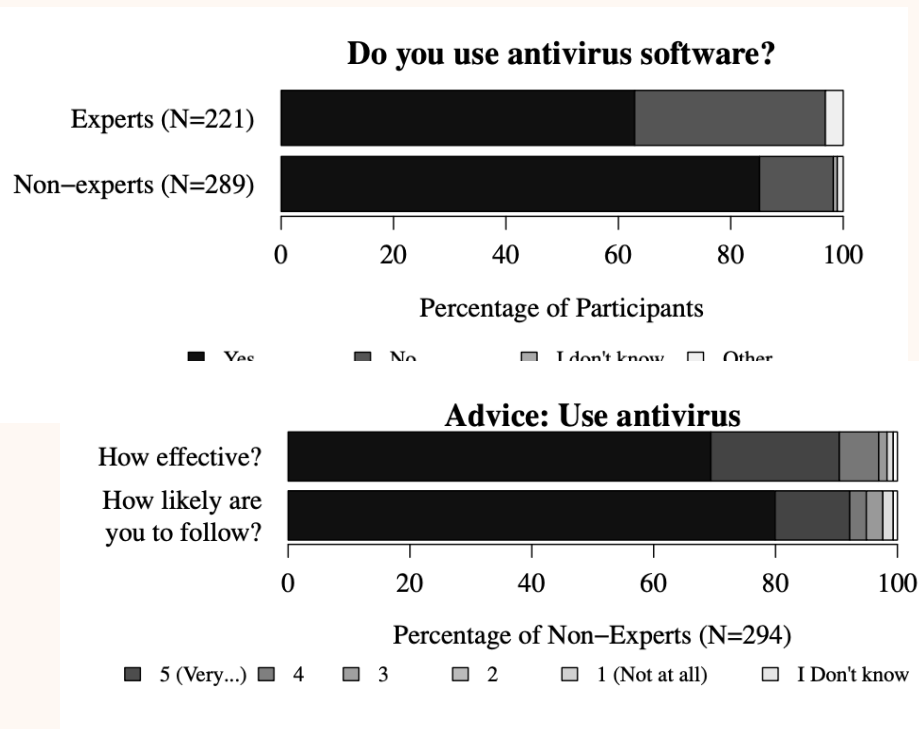
- Types of security behaviors
 - Security updates
 - Bundled with undesirable features; not sure about the benefits of it...
 - Antivirus software
 - Whether people install and how they configure it
 - Account security
 - Password use...
 - Mindfulness
 - Website visits; email habits; phishing notices...

Gap in security literacy and behavior



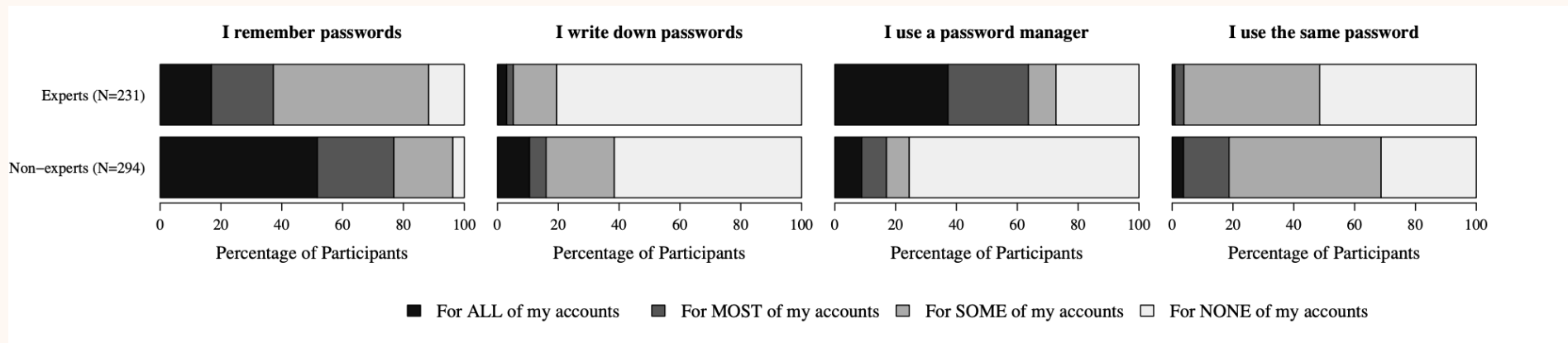
- Non-experts consider installing security updates not effective, but they will likely to follow if they heard it was effective

Gap in security literacy and behavior



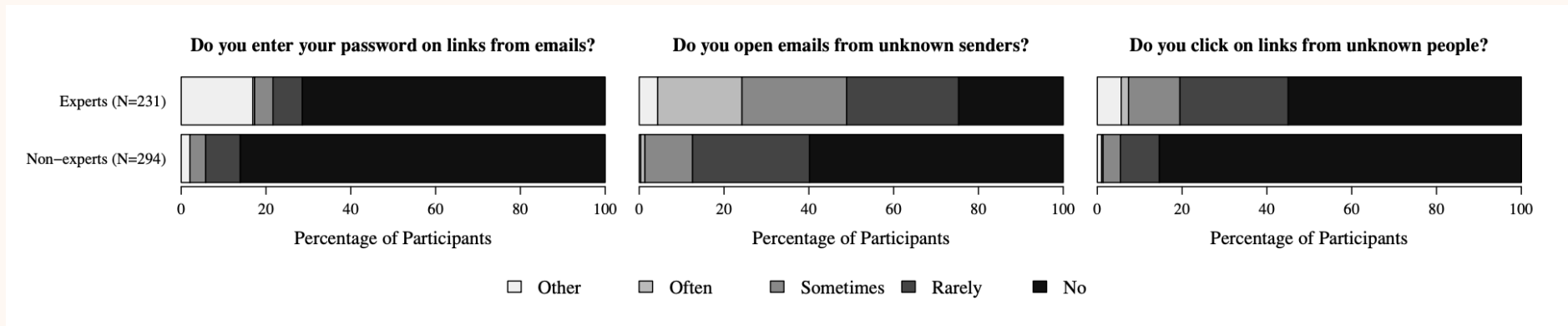
- More non-experts use anti-virus software than experts and consider it very effective – likely because it is a one-stop solution for them

Gap in security literacy and behavior



- More experts mention *strong password*, using *password manager*, and *two-factor authentication*; more non-experts mention using unique password and changing password frequently
- Only one expert mentions writing down passwords is fundamentally bad

Gap in security literacy and behavior



- Paradoxically, more experts clicks on links from unknown senders than non-experts
- Other mindfulness aspects include checking HTTPS, clearing browser cookies, and email habits.

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES

VS

SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES

1. USE ANTIVIRUS SOFTWARE



2. USE STRONG PASSWORDS



3. CHANGE PASSWORDS FREQUENTLY



4. ONLY VISIT WEBSITES THEY KNOW



5. DON'T SHARE PERSONAL INFORMATION



1. INSTALL SOFTWARE UPDATES



2. USE UNIQUE PASSWORDS



3. USE TWO-FACTOR AUTHENTICATION

2

4. USE STRONG PASSWORDS



5. USE A PASSWORD MANAGER



<https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html>

**How to read and review (USEC)
research paper?**

Where should I look for them?

*(*it's not an exhaustive list below)*

- Computer security and privacy
 - IEEE Symposium on Security and Privacy
 - USENIX Security Symposium
 - ACM Computer and Communications Security Conference
 - Network and Distributed System Security (NDSS) Symposium
- Human computer interaction
 - ACM Conference on Human Factors in Computing Systems (CHI)
 - ACM Conference on Computer Supported Cooperative Work (CSCW)
- More dedicated USEC and privacy conferences
 - USENIX Symposium on Usable Privacy and Security
 - Privacy Enhancing Technologies Symposium (PETS)

How do I read a paper?

*(*you may have more personalized way to read them)*

- Understanding what is the problem being solved and the impact?
 - Title, abstract, and introduction
- What are the (technical) innovation being made?
 - Method and design
- What are the state-of-arts and competing solutions?
 - Related work and evaluation
- What are the future (research and practical) implications?
 - Discussion

Start from the high-level ideas, dig into interesting details, iterate and reflect on them.

How do I write a review/blog?

- Summary of the work and your overall comments
- Strengths and weakness of the work; give clear, specific, and **constructive** arguments
 - Motivation and focus: if it is relevant/new/too board or too narrow?
 - Technical contribution: if it's important/applicable/useful/done properly?
 - Evaluation: if it considers relevant metrics/related baselines/is consistent and clear?
 - Writing and presentation: if it's easy to read regarding structure, notation, examples...?
 - Related work: if it is sufficient/biased?
- Suggestions to improve: based on the above, what can be improved?
- Discussion (for the blog): what's your idea for future research?

Let's practice it through the blog :)

How do I write a review/blog?

- We don't have a fixed format for news blogs, and the general idea is to stimulate further thinking and discussion.
 - Summary of the news and your overall comments
 - Why are you interested in this news?
 - Discussion (for the blog): what's your idea for future research?
 - What is the problem you are trying to understand/solve and why it is important?
 - What can be a potential solution, and what's your hypothesis?
 - A plan for testing out the solution?
- *Let's practice it through the blog :)**

Take-home

- Munyendo, C., Acar, Y. and Aviv, A.J., 2023, May. “In Eighty Percent of the Cases, I Select the Password for Them”: Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy*.
- Forbes- Warning As 1Password, DashLane, LastPass And 3 Others Leak Passwords
<https://www.forbes.com/sites/daveywinder/2023/12/11/android-warning-1password-dashlane-lastpass-and-others-can-leak-passwords/>