Prioritizing Security Practices via Large-Scale Measurement of User Behavior

Ariana Mirian
April 21, 2023
The Internet is not a safe place
Security technologies have made the Internet safer
Many attacks exploit the human in the loop
Many attacks exploit the human in the loop

Verizon Data Breach report indicates that 82% of attacks involved “The Human Element”

Technology isn’t the end answer – we need to account for the human in the loop as well

Users also have limited time and energy
Understanding user behaviors via large-scale empirical measurement can help us better prioritize security processes.
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Security “Best” Practices

- Antivirus
- Use HTTPS
- Use Mainstream OS
- Quickly Update
- Avoid Risky Sites
Security “Best” Practices

Quickly Update
Use HTTPS
Avoid Risky Sites

“...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 are. 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...
How **effective** are best practices at mitigating compromise?
Anonymized Network Traffic
Anonymized Network Traffic

Ground Truth about device compromise
Full Traffic Flows from Residential Network

Anonymized and annotated with additional metadata
Full Traffic Flows from Residential Network

Anonymized and annotated with additional metadata

Labeled with ground truth data on compromise
Full Dataset

6 months of data: 15,291 desktop/laptops, 682 (4.5%) compromised

<table>
<thead>
<tr>
<th>Security Practices</th>
<th>Applications</th>
<th>Network Usage</th>
<th>Type of Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>Browser Updates</td>
<td>Time online</td>
<td>Desktop/Laptop</td>
</tr>
<tr>
<td>Mainstream OS</td>
<td>Peer-To-Peer</td>
<td>TLD usage</td>
<td>Mobile</td>
</tr>
<tr>
<td>OS Updates</td>
<td>Flash</td>
<td>Traffic profile</td>
<td>IoT</td>
</tr>
</tbody>
</table>
Full Dataset

6 months of data: 15,291 desktop/laptops, 682 (4.5%) compromised

<table>
<thead>
<tr>
<th>Security Practices</th>
<th>Applications</th>
<th>Network Usage</th>
<th>Type of Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>Browser Updates</td>
<td>Time online</td>
<td>Desktop/Laptop</td>
</tr>
<tr>
<td>Mainstream OS</td>
<td>Peer-To-Peer</td>
<td>TLD usage</td>
<td>Mobile</td>
</tr>
<tr>
<td>OS Updates</td>
<td>Flash</td>
<td>Traffic profile</td>
<td>IoT</td>
</tr>
</tbody>
</table>
Best Practice: Use a Mainstream OS
Best Practice: Use a Mainstream OS

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Incidents</th>
<th>Total Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>538 (7.0%)</td>
<td>7,668</td>
</tr>
<tr>
<td>Mac OS</td>
<td>140 (1.9%)</td>
<td>7,339</td>
</tr>
<tr>
<td>ChromeOS</td>
<td>1 (0.5%)</td>
<td>205</td>
</tr>
<tr>
<td>Linux Variant</td>
<td>3 (3.8%)</td>
<td>79</td>
</tr>
</tbody>
</table>
Best Practice: Use a Mainstream OS

Baseline compromise: 4.5%

Windows 3.8x incident rate vs. Mac
Best Practice: Use a Mainstream OS

Baseline compromise: 4.5%

Windows 3.8x incident rate vs. Mac

Having a mainstream OS may make a user more susceptible to compromise because that’s what attackers are targeting.
Best Practice: Update Operating System
Best Practice: Update Operating System

Software Update Delay for Operating Systems

- Mac OS X
- Windows

- Clean Mean
- Compromised Mean

Delay updating OS in number of days
Best Practice: Update Operating System

Software Update Delay for Operating Systems

- Clean Mean
- Compromised Mean

No strong difference in update rate
Best Practice: Update Browsers

Software Update Delay for Browsers

<table>
<thead>
<tr>
<th>Clean mean</th>
<th>Compromised mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>Firefox</td>
</tr>
<tr>
<td>Delay (in number of days)</td>
<td>Delay (in number of days)</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Clean devices update slower than their compromised counterparts; statistically significant
Best Practice: Update Browsers

Chrome Updates: Compromised Devices

[Bar chart showing days taken to update compared to number of devices, with two sets of bars: Before Compromise and After Compromise.]
Best Practice: Update Browsers

Chrome Updates: Compromised Devices
Best Practice: Update Browsers

Chrome Updates: Compromised Devices

Compromised devices update faster after compromise
End User Behavior and Relation to Outcome

Examined best practices like using a mainstream OS and updating software

Found little empirical basis for best practices

Best practices can help, but we should prioritize behaviors that matter
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Organizations sometimes change security policies
Organizations sometimes change security policies

Adoption of 2FA

Migration to new service

Changing passwords
Organizations sometimes change security policies

Adoption of 2FA

Migration to new service

Changing passwords
What communication mechanisms are most effective at prompting user change?
Password Update Data

Possible because of collaboration with ITS Security team

Logs of password updates, employee metadata, scrambled accounts

Communication messages and when they were sent
10K Employees
10K Employees
10K Employees

Set of Four Weekly Emails
As part of our commitment to protect the UC San Diego community's data and systems, we are undergoing a campuswide password change action. Ensuring your passwords are strong is critical to protecting both your personal data and campus resources.

In addition to enhanced password security features, the minimum number of characters required for an AD password has been increased from 7 to 12 or more characters.

To meet the new minimum 12-character requirement, the UC San Diego Office of Information Assurance has begun requiring that all AD account holders make a one-time change of AD passwords after August 3, 2021.

How Do I Change My AD Password?
Successfully changing your AD password depends on the devices you are using and your location. Visit How to Change Your AD Password for more information and steps to reset devices and workstations.

Do I Have to Change My AD Password?
Yes, you are required to change your AD password, even if your current password is 12 or more characters in length.

Note that this change does not affect Business Systems SSO accounts.

When Do I Change My AD Password?
Campus academics, staff and affiliates whose last names begin with H through N are required to change AD passwords any time between September 1 and September 22.

All campus academic, staff, affiliate, Health Sciences and UC San Diego Health AD account holders have been split into groups, each group assigned dates for password changes. See the list of all groups and their assigned change dates.

The LastPass Password Management Tool
Improve password security for all of your university accounts with the UC San Diego tested and approved LastPass password management software. Visit LastPass.ucsd.edu to learn more and register.
10K Employees

Set of Four Weekly Emails

Active SSO/Email Reminders
SINGLE SIGN-ON (V3.3)

AD Password Change Required
You are required to change your AD password by 11/17/2021.

Change AD Password  Continue Log In
10K Employees

Set of Four Weekly Emails → Active SSO/Email Reminders → Scramble
Proportion of Change Modalities

81.3% are single change users

12.2% are multiple change users

5.42% are scrambled users
Each color represents a wave and the number of users who have not changed their password.
Each color represents a wave and the number of users who have not changed their password.

Solid vertical lines matching color of waves represent initial email communication.
Each color represents a wave and the number of users who have not changed their password.

Solid vertical lines matching color of waves represent initial email communication.
Each color represents a wave and the number of users who have not changed their password.

Solid vertical lines matching color of waves represent initial email communication.

Solid vertical red line represents the start of the SSO Active Directory intercept.

(a) Number of users in each wave
Each color represents a wave and the number of users who have not changed their password.

Solid vertical lines matching color of waves represent initial email communication.

Solid vertical red line represents the start of the SSO Active Directory intercept.

Solid black/grey lines represent the start of final email communications (SSO intercept active).
Period during initial email waves is categorized as “responsive period”
Period during initial email waves is categorized as “responsive period”

Period in between communications is categorized as “idle” period
Period during initial email waves is categorized as “responsive period”

Period in between communications is categorized as “idle” period

Period during SSO intercept/final email communications is the “interventional” period
Repetitive emails are useful but have potential diminishing effectiveness

(a) Number of users in each wave
Repetitive emails are useful but have potential diminishing effectiveness

“Idle” period produces little change in users
Repetitive emails are useful but have potential diminishing effectiveness.

“Idle” period produces little change in user.

SSO is most effective communication with ~80% user change rate in isolated period.
Why do users lag in their update behavior?

Examine a user’s organizational unit and relate it to their change status

Organizational unit is a proxy for someone’s department on campus
Users in Extensions, Instructors, and Extension Business are significantly overrepresented in the non-responsive user population.
Why do users lag in their update behavior?

Repeated same analysis for single change users

Examined relation between organizational unit and when user changed
Why do users lag in their update behavior?

Repeated same analysis for single change users

Examined relation between organizational unit and when user changed

Building services, Recreation, and Dining services are over-represented in the intervention period

Users in peripheral organizations take more time to respond
Organizational Effective Communication

SSO is the most effective communication mechanism, email still useful

Peripheral users might not use same communication mechanisms as other units on campus, and thus lag in their update behavior

Lessons can and have been used for future policy changes
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Email accounts are rich in information...
Defenses have made large scale attacks difficult

What are your hopes and dreams?
Targeted attacks remain an issue
Targeted attacks remain an issue
Underground markets provide hack services for hire.

- YANDEX.RU: Взлом Yandex почты (₽6990 / $107)
- RAMBLER.RU: Взлом Rambler почты (₽9990 / $152)
- GMAIL.COM: Архив Gmail почты (₽24990 / $385)
“Hack for hire” market not yet examined
How large is the market?

How sophisticated are the methods of attack?

How widely used are these services?
Focus on Gmail, but results can be generalized
Overview of process

- Discover Service
- Create Online Personas
- Engage as Buyer
- Deliver payment
- Monitor Attacks
How large is the market?

How sophisticated are the methods of attack?

How widely used are these services?
Breakdown of 27 services

- 10 never responded
- 12 responded, made no attempt (3 were scams)
- 5 made an attempt
How large is the market?

How sophisticated are the methods of attack?

How widely used are these services?
How sophisticated are the methods of attack?

We never observed: brute force logins, communication outside of email
How sophisticated are the methods of attack?

We never observed: brute force logins, communication outside of email

One service sent malware executable that wouldn’t run
How sophisticated are the methods of attack?

We never observed: brute force logins, communication outside of email

One service sent malware executable that wouldn’t run

Four of the five services used phishing in their attacks
Phishing attacks were persistent and personalized
Phishing attacks were persistent and personalized
Targeted attacks were able to bypass 2FA

Most phishing attacks accounted for 2FA in their phishing flow
One account. All of Google.

Sign in to continue to Gmail

Password
Wrong password. Try again.
Sign in
Forgot password?
One account. All of Google.

Sign in to continue to Gmail

Verify it's you

There's something unusual about how you're signing in. To show that it's really you, complete the task below.

Confirm the phone number you provided in your security settings: (**) 111175

Enter phone number

Done

Try another way to sign in
Targeted attacks were able to bypass 2FA

Most phishing attacks accounted for 2FA in their phishing flow

Phishing attempts that did not anticipate 2FA adapted

One service doubled the price of their contract upon finding 2FA
How large is the market?

How sophisticated are the methods of attack?

How widely used are these services?
Automation allowed us to fingerprint services

Much of functionality was quick and real-time

Analyzed metadata of logins to create an fingerprint for three services

Fingerprinting of automated framework allowed us to view reach of services
Hundreds of people are affected by these services
Gmail defenses introduced against MITM phishing

Better protection against Man in the Middle phishing attacks
April 18, 2019

Posted by Jonathan Skelker, Product Manager, Account Security

We're constantly working to improve our phishing protections to keep your information secure. Last year, we announced that we would require JavaScript to be enabled in your browser when you sign in so that we can run a risk assessment whenever credentials are entered on a sign-in page and block the sign-in if we suspect an attack. This is yet another layer of protection on top of existing safeguards like Safe Browsing warnings, Gmail spam filters, and account sign-in challenges.

However, one form of phishing, known as "man in the middle" (MITM), is hard to detect when an embedded browser framework (e.g., Chromium Embedded Framework - CEF) or another automation platform is being used for authentication. MITM intercepts the communications between a user and Google in real-time to gather the user's credentials (including the second factor in some cases) and sign in. Because we can't differentiate between a legitimate sign in and a MITM attack on these platforms, we will be blocking sign-ins from embedded browser frameworks starting in June. This is similar to the restriction on webview sign-ins announced in April 2016.


Increase in price for services since study finished

$24990 → $49990

$385 → $770
Hack for hire attacker characterization

Sophisticated attackers can bypass 2FA via phishing

Persistent attacks span up to multiple weeks

Successful services affect roughly 1 in a million Gmail users
Understanding user behaviors to better prioritize security processes
Understanding user behaviors to better prioritize security processes
Understanding user behaviors via large-scale empirical measurement can help us better prioritize security processes
Understanding user behaviors to better prioritize security processes

- Training Efficacy
- Vulnerability Remediation
- SETA

- HTTPS longtail
- Web Feature Deprecation
- Device Differentiation
- DPI Risks

- Attackers
- Organization
- End Users
Thank you
A Counter-Roast
A story
Thank you!!
Thank you
Questions?

arianamirian.com
arianamirian28@gmail.com
@arimirian
@amirian@infosec.exchange