Account Protections
a Google Perspective

Elie Bursztein
Google, @elie

with the help of many Googlers

updated March 2021
Slides available here:
https://elie.net/account
4 in 10
US Internet users report having their online information compromised

Source: the United States of P@ssw0rd$ - Harris / Google poll
How do attacker compromise accounts?
Main source of compromised accounts

- Data breach
- Phishing
- Keyloggers
The blackmarket is fueling the account compromised ecosystem.
Accounts and hacking tools are readily available on the blackmarket.
Volume of credentials stolen in 2016: a lower bound

- Data breach: 4.3B+
- Phishing: 12M+
- Keyloggers: 1M+

[Google Security and Privacy Group](https://security.google.com)

Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. CCS'17
Stolen credential origin takeaways

- The black market fuels account compromise
- Password reuse is the largest source of compromise
- Phishing and keyloggers poses a significant risk
How can we prevent account compromise?
Defense in depth leveraging many competing technologies
Increasing security comes at the expense of additional friction including lock-out risk, monetary cost, and user education.
Each security solution offers a different trade-off which makes security a complex balancing act between usability and security.
Credentials are stolen
Stolen credential database is built
Accounts are compromised
At risk users face advanced attacks

Preventing credential theft
Resetting leaked credentials proactively
Preventing unauthorized login
Advanced protection

Today: combining key technologies to offer the best account security and usability possible
Part 1
Preventing credentials theft
Build large scale AI powered systems to detect and block threats at scale before they reach users.
Safe Browsing warnings protects over 4 billions devices from phishing, malware
Millions of warnings displayed weekly

https://transparencyreport.google.com/safe-browsing/overview
Attackers are shifting to phishing

https://transparencyreport.google.com/safe-browsing/overview
Everyday Gmail blocks over 100M+ phishing emails
Cats through the age

- 2000 BC
- 1200 AC
- 1800 AC
- 2020 AC
Drive phishing through the ages
68% of phishing emails blocked by Gmail are different from one day to the next.
Keeping up with constantly evolving attacks requires continuously improving and retraining detection systems. As in evolution the red queen hypothesis applies: it takes all your running to stay ahead of attackers.
How to deal with a borderline case?
Provide as much context as possible and rely on user to make the final decisions.
Gmail inbox soft warnings help users decide which emails are phishing
45% of Internet users don’t know what phishing is
Takeaways

Prevention is a critical first defense layer
It protects billion of users across the world from being phished and infected

Keeping up with attack evolutions requires constant improvements
Attackers actively attempt to evade detection that are major hurdles to them

Education and warning design are a must
Make sure that users understand the risks and don’t get warning fatigue is very challenging
Section 2

Resetting compromised credentials proactively
Third party data breaches keep surfacing

Dropbox data breach: 68 million user account details leaked

LinkedIn Lost 167 Million Account Credentials in Data Breach

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack
66% Of US users reuse passwords across online services

Source: the United States of P@ssw0rd$ - Harris / Google poll
59%
Of the U.S. adults use a name or a birthday into some of their online password

Source
The United States of P@ssw0rd$ - Harris / Google poll
Get users to use a password manager
15% of US Internet users use a password manager. 36% use a piece of paper.

Source
The United States of P@ssw0rd$ - Harris / Google poll
We need additional defenses to mitigate password reuse until password managers are ubiquitous.
Cleaning up after password dumps
September 10, 2014

One of the unfortunate realities of the Internet today is a phenomenon known in security circles as “credential dumps”—the posting of lists of usernames and passwords on the web. We’re always monitoring for these dumps so we can respond quickly to protect our users. This week, we identified several lists claiming to contain Google and other Internet providers’ credentials.

Disclosing the existence of our proactive breach password reset program
110M+
Google accounts proactively re-secured
How to protect all internet accounts against compromised password reuse?
Ideal password warning system properties

- Privacy preserving
- Accurate & actionable
- Automated
Private set intersection

Allows users to query Google about the breach status of their usernames and passwords without revealing the information queried.
Additional cryptographic mechanism ensure that malicious actors can’t use the system to learn leaked username and password.
Password Checkup protects hundreds of millions of users from leaked passwords by displaying tens of millions of warnings weekly.

https://blog.google/technology/safety-security/keeping-private-information-private/
100M+ people have used Password Checkup, and they’ve seen a 30% reduction in breached credential usage

https://blog.google/technology/safety-security/keeping-private-information-private/
Password check up on android

Predictive anti-phishing protection

https://security.googleblog.com/2021/02/new-password-checkup-feature-coming-to.html
Takeaways

Proactive password protections greatly reduce malicious sign-in
People all too often choose easy to guess passwords

Password manager can solve a lot of those issues
Get users to realize how important this is for them
Section 3
Preventing unauthorized logins
Password only authentication is dangerous
Use additional information

To prevent hackers logging in with compromised credentials
Types of additional information

Who you are

What you have

What you know
Mass adoption of two factor authentication is challenging.
37% of US internet users use two-factor authentication.

Source: The United States of P@ssw0rd$ - Harris / Google poll
52.5% of the online service don’t offer two factor authentication

Source:https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild/
Some industries don’t use standards

Many sites marketing reuse terminology incorrectly and end-up confusing users

Which type of two factor authentication should we push for?
Not all 2FA technologies are equal

<table>
<thead>
<tr>
<th></th>
<th>Secondary email</th>
<th>SMS verification</th>
<th>Device prompt</th>
<th>Security key</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boutique phishing</strong></td>
<td>68%</td>
<td>96%</td>
<td>99%</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Spear-phishing</strong></td>
<td>53–100%</td>
<td>76%</td>
<td>90%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Source: Evaluating Login Challenges as a Defense Against Account Takeover - WWW19
Security keys are the most secure second factor against phishing.

- Physical key
- Security key built into your phone
How to speed up security key adoption?
Say hello to OpenSK an open-source security key written in RUST
OpenSK: Design Philosophy

Open
Open source, no patents, no NDAs, affordable.

Secure by design
Memory-safe programming language, and secure OS.

Research friendly
Cheap & easy to audit your own key, and attack it.
OpenSK: hardware

TockOS

Nordic chip

Case 3D blueprint
Paul Rascagnères @r00tbsd · Jan 30

New open source project from Google: **OpenSK**. A FIDO U2F and FIDO2 implementation for Nordic nRF52840 board. I'm not an expert but it looks like a #yubikey but with an open source firmware and 5 times cheaper... and great STL files to 3D print the case ;) github.com/google/OpenSK/...
Help manufacturing OpenSK-based affordable security key for everyone

Since Feb’21 Feitan OpenSK research edition key available on Amazon for $9.90 (not ready for production!)
What’s next? Major milestones

1. **FIDO 2.1 Certification**
   - OpenSK on track to be the first FIDO 2.1 certified key

2. **Bleeding edge features**
   - New features to make keys more secure and usable are actively developed

3. **Improved manufacturing**
   - Keep partnering with the industry to develop high quality affordable security keys
More information at:
https://github.com/google/opensk
Takeaways

Password are not enough
Password reuse and phishing makes credentials only login very risky

Strong two factors is the way to go
Not all 2nd factors are created equals we need to focus on strong two factor adoption

Industry wide adoption is still very distant
There are a lot of structural problem to solve before we get 2FA as universal as HTTPS
Section 4
Advanced protection
Large scale attacks don’t care which accounts they target
Personalization

Targeted attacks
Resourceful attackers that target specific individuals and organizations

Boutique hacking
Hand-crafted campaigns targeting a few dozen individuals or organizations

Bulk hacking
Automated campaigns targeting many individuals and organizations
Accounts at risk of targeted attacks

- Journalists & hacktivists
- Politicians & campaign teams
- Executives & Fintech users
- Celebrities
Key threats faced by targeted users

Spear-phishing

Handcrafted phishing attacks with two factor phishing is a common tactic against targeted users

Malicious oauth app

Attackers use oauth app to maintain persistent access to targeted users

Advanced account recovery impersonation

Attackers research their target background and use the collected data for impersonation and phishing purpose
Realtime password verification and then phishing the SMS code
Increase security further at the expense of additional friction
Lock-down login
Mandatory security keys

Protecting Session
Limit API Data Access

Protecting Session
Squeeze out malware

Account Recovery
Stronger Verification
Takeaways

- Strong account security requires a defense in depth strategy
- Constant improvements are needed to keep-up with adversaries
- Additional protections are need for targeted users
Effective account security requires tailoring your protections to meet your users needs

https://elie.net/account