Account Protections
a Google Perspective

Elie Bursztein
Google, @elie

with the help of many Googlers
4 in 10 US Internet users report having their online information compromised

Source: the United States of P@ssw0rd$ - Harris / Google poll
How do hackers 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+
Stolen credentials volume

Data breach

Keyloggers

Phishing

Targeted attack

Risk

Google Security and Privacy Group
Stolen credential origin takeaways

The black market fuels account compromise

Password reuse is the largest source of compromise

Phishing pose significant risk
How can we prevent account compromise?
Why do we need many counter-measures?
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.
Today: disrupting the account compromise cycle

- **Credentials are stolen**
- **Stolen credential database is built**
- **Accounts are compromised**
- **At risk users face advanced attacks**

- Preventing credential theft
- Resetting compromised credentials proactively
- Preventing unauthorized login
- Advanced protection
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 protect over 3 billion 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 the phishing emails blocked by Gmail are different from day to day.
Keeping up with constantly evolving attacks requires a continuously improving detection system and very fast retraining. 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.
2014
Disclosing the existence of our proactive breach password reset program
110M+
Google accounts proactively re-secured
How to protect all 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

We analyzed your saved passwords and found the following issues:

1. **2 compromised passwords**
   - Change these passwords now
   
   This account is at risk
   
   ![DriveNow Carsharing](image)
   
   ![microsoft.com](image)
   
2. **15 reused passwords**
   - Create unique passwords

3. **21 accounts using a weak password**
   - Create strong passwords

Change these passwords now

The following account credentials were found to be exposed in a third-party data breach. Change these at-risk passwords immediately to keep your accounts safe. Learn more.

This account is at risk

![DriveNow Carsharing](image)

![microsoft.com](image)
Password checkup protect hundreds of millions of users from leaked passwords by displaying tens of millions of warnings weekly.
How about phishing attacks?
Phishing predictive protection

https://www.blog.google/products/chrome/better-password-protections/
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

https://elie.net/blog/security/the-bleak-picture-of-two-factor-authentication-adoption-in-the-wild
47.5% 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>Security level</th>
<th>Secondary email</th>
<th>SMS verification</th>
<th>Device prompt</th>
<th>Security key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boutique phishing</td>
<td>68%</td>
<td>96%</td>
<td>99%</td>
<td>100%</td>
</tr>
<tr>
<td>Spear-phishing</td>
<td>53-100%</td>
<td>76%</td>
<td>90%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Evaluating Login Challenges as a Defense Against Account Takeover - WWW19
Security keys are the most secure second factor against phishing.
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.
Google device security research in Zurich
OpenSK developer edition
More information here:
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
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 needed for targeted users**
Effective account security requires tailoring your protections to meet your users needs

https://elie.net/fic20