The Anatomy of Account-Takeover

Grzegorz Milka (grzegorzmilka@google.com)
Online accounts are valuable targets

- Financial data
- Personal data
- Contacts
- Identity (impersonation)
Data breaches are always there

Dropbox data breach: 68 million user account details leaked

Yahoo Says 1 Billion User Accounts Were Hacked

LinkedIn Lost 167 Million Account Credentials in Data Breach
And so are targeted hijacks

https://techcrunch.com/2017/08/23/i-was-hacked/
We want to protect all users, and today we discuss passwords.
Modern password authentication requires a risk-aware, defense-in-depth system.
Password theft ecosystem
The three avenues of password theft

- Data breach
- Malware (Keyloggers)
- Phishing
Commoditization of abuse
The wares on sale

Data breach market

Keyloggers

Phishing kits
Markets can be tracked

In 2016, we have collected over 4000 data breach dumps with over 3.3B credentials.
Users reuse passwords

12%-43%*

reuse rate

*“Data breaches, phishing, or malware?”

Research at Google
Users reuse passwords

17%*

reuse rate

* internal estimate
Number of valid Google passwords found in data breaches:

67 Million
Volume of credentials stolen in 2016*

Data breaches >3.3B
Keyloggers >1M
Phishing >12M

*all services, lower bound
Hijacking likelihood*

Compared to a general active account, how much more likely it is that you will be a victim of hijacking if we know:

- >10x: You were in a breach
- >40x: Had a keylogger
- >500x: Were phished

*lower bound
Prevention

Sign-in risk detection

Challenges
Modern password authentication requires a risk-aware, defense-in-depth system.
Safe Browsing

Deceptive site ahead

Attackers on esty.adelawarriewood.com.au may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

✓ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

DETAILS  Back to safety
We notify compromised users and ask them to change their password.
Prevention
Sign-in risk detection
Challenges
Password-only authentication is risky.
Adoption of additional security is low

<10%  2FA

~12%  Password managers*

Of active Google accounts

Of Americans *Pew Research Center
Sign-in risk detection

Image courtesy of Dr Frank Stajano, “Passwords and the Evolution of Imperfect Authentication”
Dimensionality of risk

How surprised we are to see you login like that?
Unusual location, device, time

How suspicious does the login look?
- Similarity to known hijacking patterns
- Is user at risk?
Hijackers adapt.
Geocloaking

$message .= "----------------+ Begin +-----------------
"
$message .= "Email : " . @$_POST['Email'] . "\n"
$message .= "Password : " . @$_POST['Passwd'] . "\n"
$message .= "---------+ IP Address & Date +---------\n"
$message .= "IP Address: " . $ip . "\n"
$message .= "Country: " . $country . "\n"
$message .= "Date: " . $adddate . "\n";

~83% phishing kits

In the end, we don’t look at user’s location for many users.
Dynamic 2FA: Ask for additional verification

When the sign-in is risky

That is solvable by the user
Modern password authentication requires a risk-aware, defense-in-depth system.
2 things that can go wrong

Hijacker gets in

User is locked out
Choose the challenge that minimizes damage

- Allow
- MAIL VERIFICATION
- SMS CODE
- GOOGLE PROMPT
- Deny
Secondary e-mail verification

10% of users have problems passing this challenge.

Research at Google
Secondary e-mail verification

Vulnerable to password reuse
SMS code

Vulnerable to phishing...

18% of observed phishing kits collect phone data.

... and other methods

There are multiple ways to get the SMS code besides phishing.
I was hacked

https://techcrunch.com/2017/08/23/i-was-hacked/
SMS code

Most successful hijackings of high-value 2FA-accounts involve breaking the SMS code.

SMS code interception happens in targeted attacks as well as in opportunistic ones.
SMS code

“by January 2016, [the number of phone hijackings] had increased to 2,658.”

Lorrie Cranor, FTC Chief Technologist
Google Prompt

Nothing stops the user from just clicking “Yes”

More flexible

We can present more data and use additional signals for risk-analysis
In-session detection
Hijacking monetization

- Theft of personal data
- Viral-phishing and scams
- Spamming and product abuse
Bringing the user into the loop

Google

Suspicious activity in your account

Hi Grzegorz,

Someone recently signed into your Google account grzegorzmlka@gmail.com and created unusual Gmail message filters.

Details:
Thursday, January 11, 2018 2:14 PM (Israel Time)
Tel Aviv-Yafo, Israel

Review your recently used devices to make sure no one else has access to your account.

REVIEW YOUR DEVICES NOW

Go to the Help Center to learn more about Gmail filters.

The Google Accounts team

*The location is approximate and determined by the IP address it was coming from.

Googlers, please file any feedback here.
This email can't receive replies. For more information, visit the Google Accounts Help Center.
Finding the hijacker in-session

20:54:24 | LOGIN (new)       |
20:55:51 | MAIL_DELETE      | 1 (new device notifn.)
Finding the hijacker in-session

20:54:24 | LOGIN (new)   |
20:55:51 | MAIL_DELETE  | 1 (new device notifn.)
21:01:30 | EXPORT_CONTACTS |
Finding the hijacker in-session

20:54:24 | LOGIN (new) |
20:55:51 | MAIL_DELETE | 1 (new device notifn.)
21:01:30 | EXPORT_CONTACTS |
21:06:45 | MAIL_SEND | with phishing links
21:07:50 | MAIL_FILTER | “hacked”->Trash
21:08:07 | LOGOUT |
Modern password authentication requires a risk-aware, defense-in-depth system.