Account Security: Passwords & 2FA

Last updated 1/20/21
Threat modeling: Why would someone want your password?
Threat modeling helps us ground our fears in reality
Context is key!

What type of work are you doing?

This affects the type of threat you’ll face.
Context is key!

What about your identity affects how you move through the world?

This can affect how severe impact of a threat will be.
## What is likely?

<table>
<thead>
<tr>
<th>INCIDENT TYPE</th>
<th>COUNT OF INCIDENTS</th>
<th>COUNT OF SAMPLE</th>
<th>% OF SAMPLE EXPERIENCE INCIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Email Phishing</td>
<td>140</td>
<td>41</td>
<td>26%</td>
</tr>
<tr>
<td>2. Malware</td>
<td>54</td>
<td>39</td>
<td>25%</td>
</tr>
<tr>
<td>3. Account Compromise</td>
<td>20</td>
<td>18</td>
<td>12%</td>
</tr>
<tr>
<td>4. Business Email Compromise</td>
<td>14</td>
<td>13</td>
<td>8%</td>
</tr>
<tr>
<td>5. Wire fraud</td>
<td>3</td>
<td>3</td>
<td>2%</td>
</tr>
<tr>
<td>6. Virus</td>
<td>1</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>7. Advanced Persistent Threat</td>
<td>1</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>8. Supply Chain</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>9. Ransomware</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>233</td>
<td>116</td>
<td>50%</td>
</tr>
</tbody>
</table>

^^ From Community IT’s 2018 Non-profit Cybersecurity Incidents Report
How to build your threat model

What has happened to the org before? What is likely to occur?

Are certain members of the org more visible/public?

Are certain members of the org experiencing harassment or stalking?

Are org members or clients a part of marginalized communities?

Who are the threat actors? Fraudsters? Extremists? State actors?

→ Ground your threats in reality, not fear
Account compromise, often through phishing, is a common attack. Why would someone want your email password?

- **Examples include...**
  - Access client/member info
  - SSNs
  - Access shared files
  - Information for an “exposé”
  - Pretend to be you & try to get money/gift cards

- **Other ideas?**
How does someone get your password?
CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET’S HOUSE.

THEM WRITHE ALL THEIR PASSWORDS IN A BOOK Labeled "PASSWORDS"!

THE FOOL!

HOW PEOPLE THINK HACKING WORKS

HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.

COOL, LET’S TRY THEM ALL ON VENMO.

HOW IT ACTUALLY WORKS
How does an attacker get your password?

- **Guessing it**
  - Dictionary attacks/brute force guessing
  - Easily searchable things about you (birthday, pets names)
- **Finding it**
  - Breach list + password reuse
- **Tricking you into divulging it**
  - Phishing
  - Social Engineering
Buying it or getting it for $free.99
Tricking you - Phishing

Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account
john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.
Threat modeling: likelihood & severity

- **Likelihood of Threat Occurring**
  - Likely

- **Severity of Threat**
  - Targeted brute force attack
  - Phishing
  - Public data breach
Could someone have your password right now??
Checking public breach lists

Let’s check a trustworthy website that lists public lists of already stolen passwords and emails.

→ haveibeenpwned.com

Pro tip!

Subscribe your email address to haveibeenpwned to get an alert if you’re in a breach!
What sites come up?

- Have you used the passwords from those sites anywhere else?
- ... Have you used those passwords at work?
Solutions: Password Security
The trick: a strong, unique password!

Passwords must be unique because of the common threat of data breaches, like the ones on haveibeenpwned.com.

What makes a password strong?
The trick: a strong, unique password!

What makes a password strong?

→ howsecureismypassword.net
How Secure Is My Password?

✔️ The #1 Password Strength Tool. Trusted and used by millions.

Your password would be cracked

Instantly
How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

It would take a computer about

8 hours

to crack your password
How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

hg7Vtzy#45fw2s

It would take a computer about

2 hundred million years

to crack your password
How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

silly brutal safe travel

It would take a computer about

3 sextillion years

to crack your password
Remembering unique, complex passwords for every account is VERY hard.

That’s why password managers exist!
What’s a password manager?
Password management services generate and hold diverse, strong passwords.
Password Managers are Convenient!
Password Managers are Secure!

- Stored securely with end-to-end encryption
- Generates random passwords
- Some password managers warn you when you have weak or reused passwords
- Enables safe sharing of sensitive information
Bonus: check for phishing!

If your password manager recognizes a site (in this case, login.gov) and you have the browser extension installed, it’ll prompt you to use the password manager to login.

If it’s a site pretending to be Login.gov, you won’t see that prompt.
When you use a password manager, you’ll have just one password to remember.

The password manager doesn’t keep a copy of this password – it is the key to unlock all your other passwords, so without it, all your information is encrypted and scrambled.

It’s really important that it be unique, long, and strong, but also something you can remember without writing it down!
Using a strong, unique password for each account + a password manager

Likelihood of Threat Occurring

- Targeted brute force attack
- Phishing
- Public data breach

Likely Severity of Threat
Key takeaway:

Do whatever you can to avoid password reuse and weak passwords!
Solutions: Multi-Factor Authentication
MFA keeps your account safe even if your password is compromised
More than your password

“2 factor” or “multi-factor” authentication

- Something I know (a good password) = good
- Something I know + something I have with me = even better!
Types of MFA

The second factor might be:

- A text to your phone
- A number in Google Auth or another authenticator app
- A yubikey or other physical key
Illustration of security key from Solo (open source security key):
How Effective is MFA? Account Takeover Prevention Rate

They mean an authenticator app!

Text message code

Hardware token like a yubikey

Device-based challenges

- On-device prompt: 100%
- SMS code: 96%
- Security key: 100%

Pro tip!
Hide notifications content from showing up when your phone screen is locked!
Using a strong, unique password for each account + a password manager

Likelihood of Threat Occurring

Targeted brute force attack

phishing

Public data breach

Likely Severity of Threat

Likelihood of Threat Occurring
Key takeaway:

Turn on MFA -- this way even if you get pwned you won’t get hacked!