SIGPwny

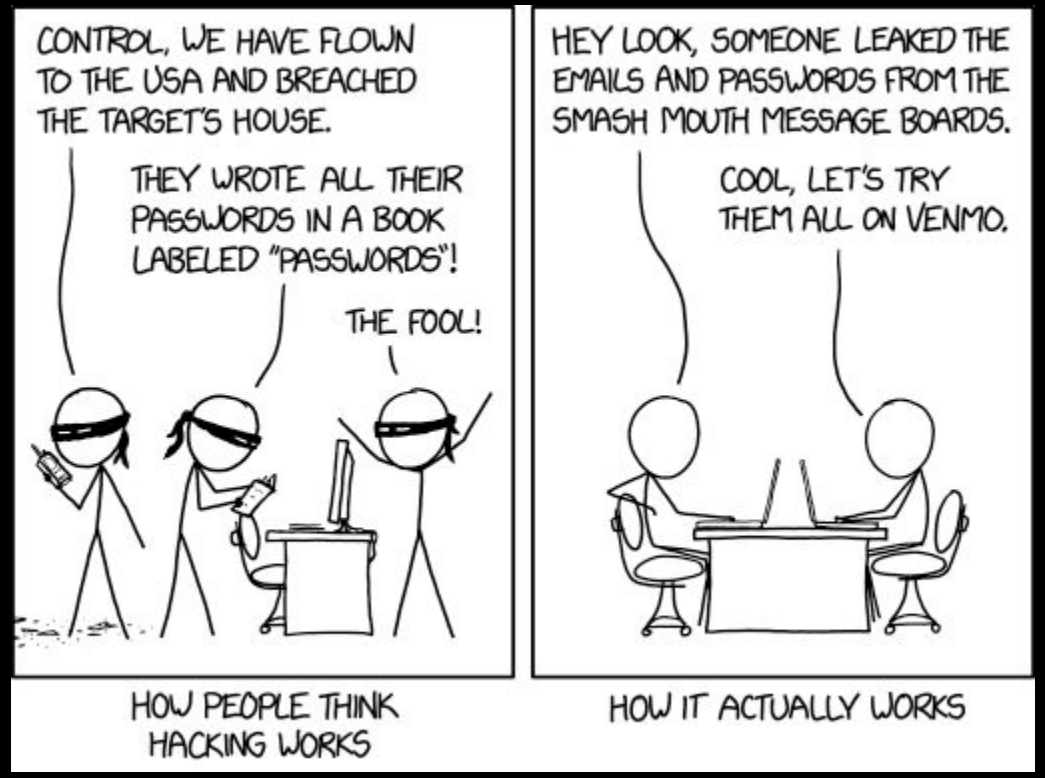
FA2024 Week 06 • 2024-10-12

Personal/Operational Security

Sagnik Chakraborty and Minh Duong

ctf.sigpwny.com

sigpwny{m4ny_ph1sh_in_th3_se4}

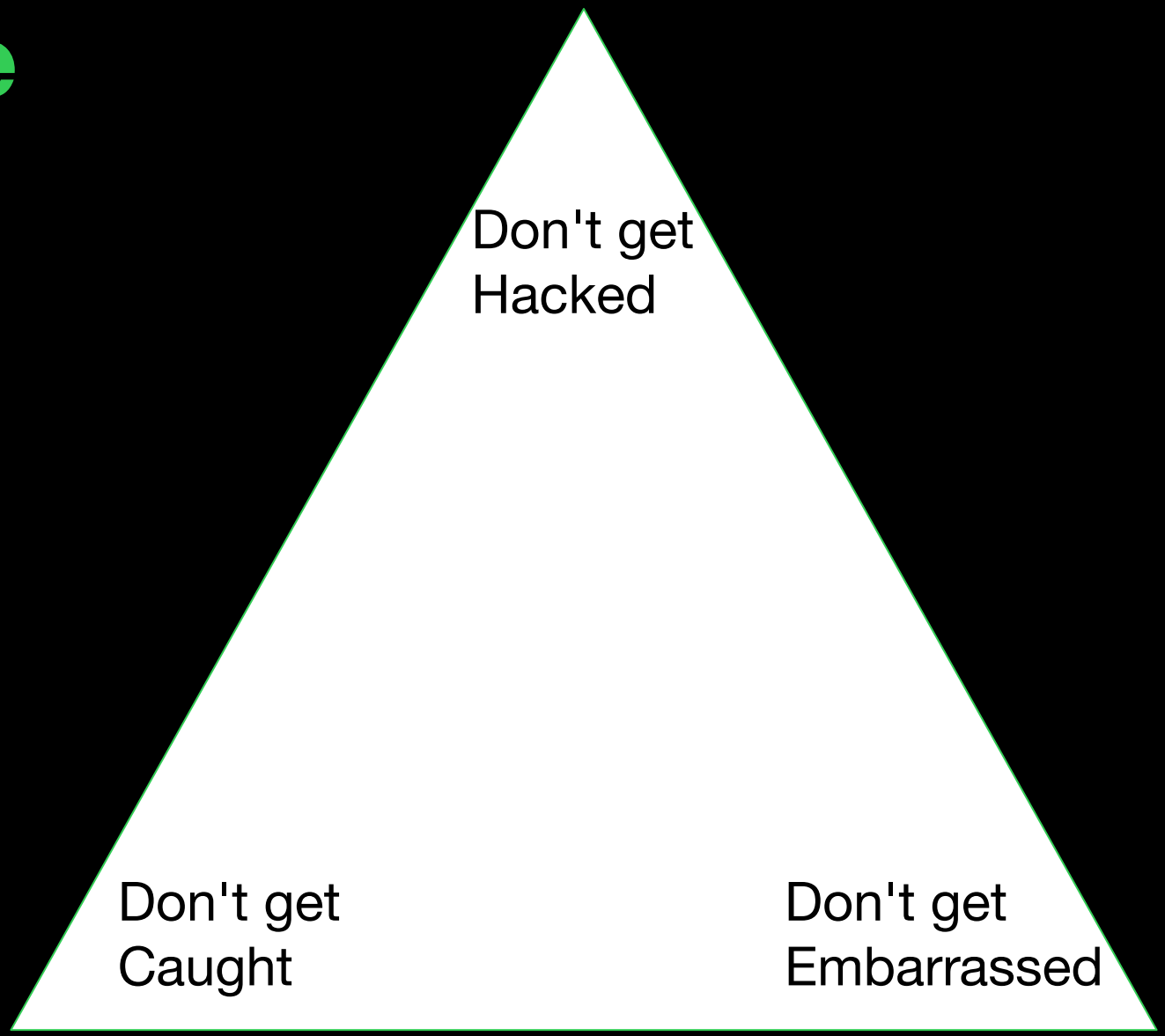


Operational Security

- *“A process that identifies critical information to determine if any actions in an operation can be caught by enemy intelligence”*

- In this meeting, we will use **OPSEC** to describe how to protect our information and enhance our privacy

The OPSEC Triangle



Don't Get Hacked

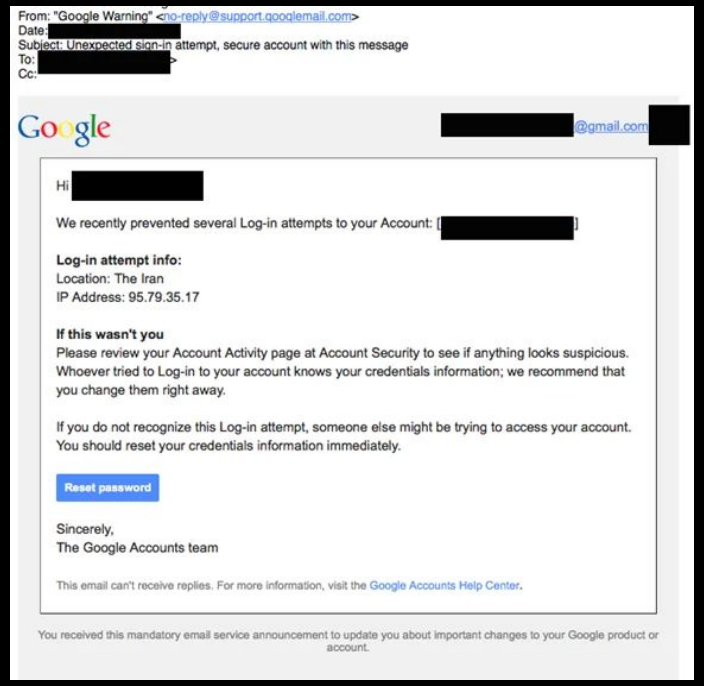
Protecting Info Checklist

- Use randomly generated passwords
  - Use special characters: `$[#!%@_`
  - *Make different passwords each time!*
- Password Manager
  - Helps you randomly generate passwords
  - Bitwarden encrypts all passwords with zero-knowledge encryption
- MFA
  - 2FA is good, SMS based is weak but better than pure password
    - In general, YubiKey > TOTP Authenticator > SMS > Only password
- Awareness
  - Be cautious of phishing links and suspicious emails ⇒ Verify the source!

Protecting Info Checklist

- Use randomly generated passwords
  - Use special characters: `$[#!%@_`
  - *Make different passwords each time!*
- Password Manager
  - Helps you randomly generate passwords
  - Bitwarden encrypts all passwords with zero-knowledge encryption
- MFA
  - 2FA is good, SMS based is weak but better than pure password
    - In general, YubiKey > TOTP Authenticator > SMS > Only password
- Awareness
  - Be cautious of phishing links and suspicious emails ⇒ Verify the source!

Protecting Info Checklist


From: "Google Warning" <no-reply@support.googlemail.com>
Date: [redacted]
Subject: Unexpected sign-in attempt, secure account with this message
To: [redacted]
Cc:

Google [redacted]@gmail.com

Hi [redacted]

We recently prevented several Log-in attempts to your Account: [redacted]

Log-in attempt info:
Location: The Iran
IP Address: 95.79.35.17

If this wasn't you
Please review your Account Activity page at Account Security to see if anything looks suspicious. Whoever tried to Log-in to your account knows your credentials information; we recommend that you change them right away.

If you do not recognize this Log-in attempt, someone else might be trying to access your account. You should reset your credentials information immediately.

Reset password

Sincerely,
The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

- Use randomly generated passwords
  - Use special characters: $[#!%@_
  - *Make different passwords each time!*
- Password Manager
  - Helps you randomly generate passwords
  - Bitwarden encrypts all passwords with zero-knowledge encryption
- MFA
  - 2FA is good, SMS based is weak but better than pure password
    - In general, YubiKey > TOTP Authenticator > SMS > Only password
- Awareness
  - Be cautious of phishing links and suspicious emails ⇒ Verify the source!

You can still be phished!

Protecting Info Checklist

- Use randomly generated passwords
  - Use special characters: `$[#!%@_`
  - *Make different passwords each time!*
- Password Manager
  - Helps you randomly generate passwords
  - Bitwarden encrypts all passwords with zero-knowledge encryption
- MFA
  - 2FA is good, SMS based is weak but better than pure password
    - In general, YubiKey > TOTP Authenticator > SMS > Only password
- Awareness
  - Be cautious of phishing links and suspicious emails ⇒ Verify the source!

Safe Browsing

- AdBlock
  - uOrigin, works like a charm, stops malicious pop ups too
- Ensure HTTPS wherever you can

- **Update software whenever possible!**

Safe Browsing

- Anonymous Search Engines
  - DuckDuckGo: doesn’t track your activity or store your personal information
  - SearXNG: Metasearch engine, also doesn't track your personal search data/history

Don't Get Embarrassed

Everything you say can and will be used against you!

Identity Models

- Level 1: You don't exist
  - Randomized, Isolated accounts whenever applicable
  - No indication of who you are, keep minimal footprint

- Level 2: You don't care

- Level 3: You are a celebrity

Identity Models

- Level 1: You don't exist

- Level 2: You don't care ← most of you
  - Most people do this one, society is becoming more accepting of this

- Level 3: You are a celebrity

Identity Models

- Level 1: You don't exist

- Level 2: You don't care

- Level 3: You are a celebrity
  - This is good for recruiters, protects against impersonation attempts
  - Watch everything you say, follow all "Don't get hacked measures"

Don't Get Caught

If you're worried about this, you're probably already up to no good. Probably.

Personal Data = Radioactive Waste

- Easy to generate in the short term
- ***Extremely*** difficult to get rid of
- Requires planning in the long term to manage correctly

Protect your Communications

- Encrypt emails
  - OpenPGP: make a public/private key pair for message sending/encrypting

- Use E2E encrypted messaging
  - Apple-to-Apple comms are E2E encrypted; messages to other devices aren't necessarily so
  - Signal (Telegram, WhatsApp aren't *really* E2E)

- Use VPNs to protect your communications
  - I use ExpressVPN generally which I've found to work quite well

Privacy

- Lock down your accounts

- Ensure Least Access
  - Who *really* needs to see your IG posts? Your LinkedIn?

- Review App Perms
  - Regularly check and remove unnecessary permissions from apps and devices

Data Brokers

- Companies that buy/collect/sell personal information
- Use privacy tools and browser extensions that block trackers
- Opt out of data collection whenever possible, and limit the amount of personal data you share online
- Remember, your personal data is your right

Edit, then delete

- Many websites will continue to store all your data after you delete your account.

- To defeat them, one thing you can do is edit the posts first and then delete

If you get caught

Know the law

Know your rights

Get a lawyer

SHUT THE HELL UP

General Tips

Risk Management

- Who are you?
  - An International Espionage Agent?
  - Drug dealer
  - Student, Security researcher
  - ACCOUNTING\John

- What are *actual* threats to you?

- Make a model
  - Spreadsheet, Graph, Drawing, etc.

Risk Management

- Who are you?
  - An International Espionage Agent?
  - Drug dealer
  - Student, Security researcher
  - ACCOUNTING\John

- What are *actual* threats to you?

- Make a model
  - Spreadsheet, Graph, Drawing, etc.

Risk Management

- Who are you?
  - An International Espionage Agent?
  - Drug dealer
  - Student, Security researcher
  - ACCOUNTING\John

- What are *actual* threats to you?

- Make a model
  - Spreadsheet, Graph, Drawing, etc.

Compartmentalization

- Don't have one email to do everything
- Also don't have *random* emails *without purpose*

- Have *different* emails with **different purposes**
  - Personal/Informal
  - Professional Email
  - `thisistotallynotadiscordalt@yahoo.com`

- Have multiple roots of trust
  - 100% going to depend on your threat model

Security Fatigue

This is going to seem tiring

There are diminishing returns

There's an inherent tradeoff between Security and convenience

Do not give up.

It’s easy to get depressed when you learn about or work in security.

Watch out for the slippery slope fallacy — just because one thing is bad doesn’t mean we should stop trying to make things better (voting records & birthdates).

Next Meetings

YYYY-MM-DD • This/Next Thursday/Sunday

- Topic
- Description

YYYY-MM-DD • This/Next Thursday/Sunday

- Topic
- Description

YYYY-MM-DD • This/Next Thursday/Sunday

- Topic
- Description

ctf.sigpwny.com

`sigpwny{m4ny_ph1sh_in_th3_se4}`

Meeting content can be found at sigpwny.com/meetings.

SIGPwny