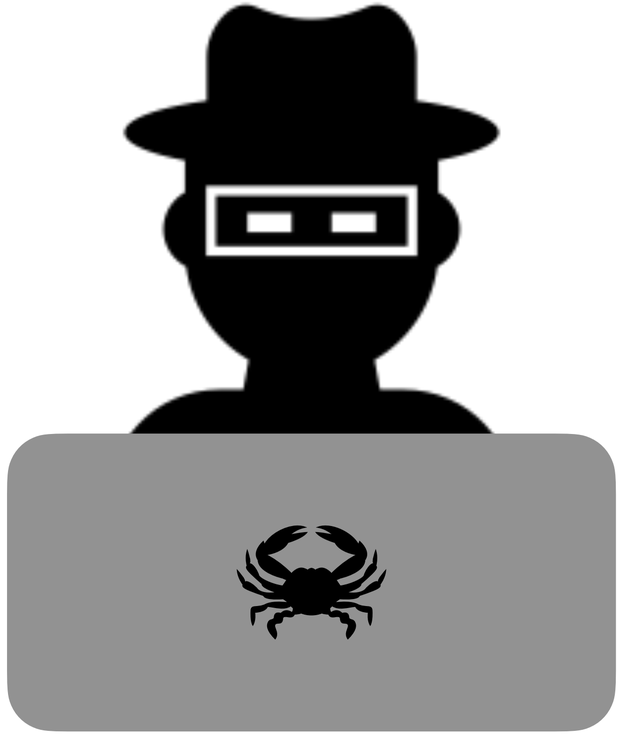
Intro to Cyber Security

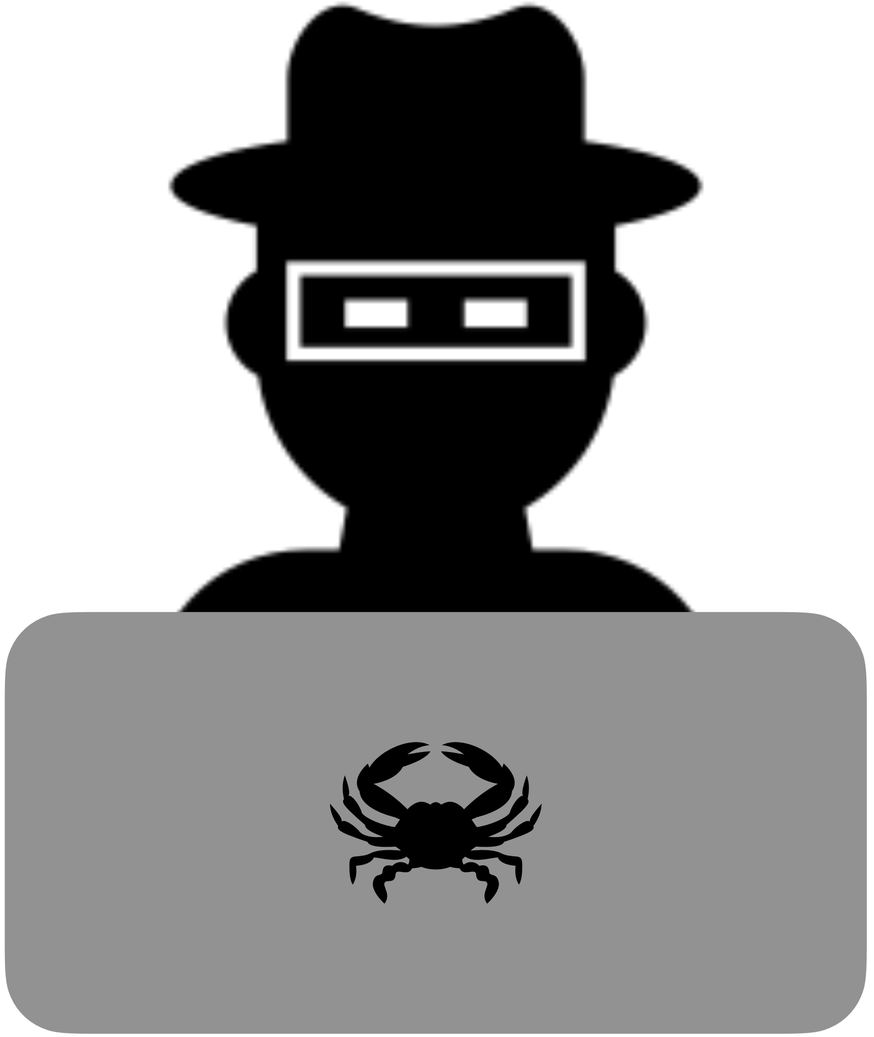
“Internet Safety Basics” @The Forum



Amitabh Garg - Oct. 28, 2021

Myth of the “Hacker”

What is a Hacker?

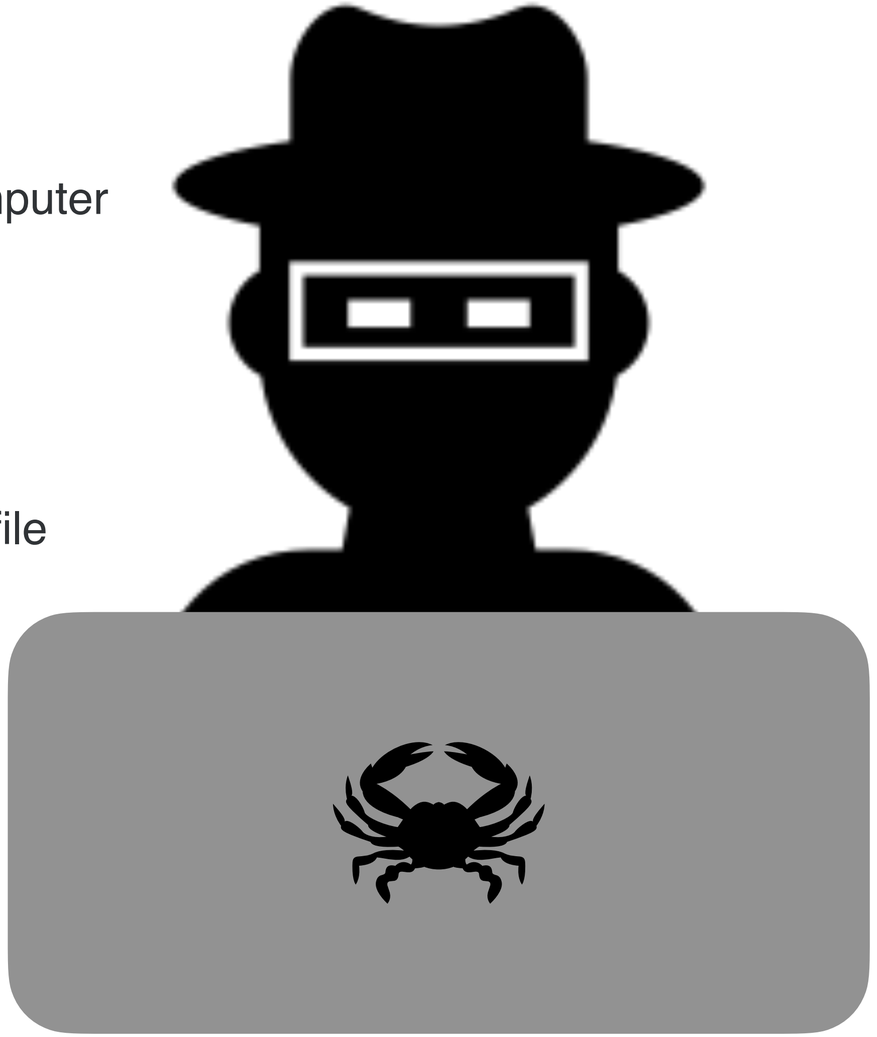


Myth of the “Hacker”

What is a Hacker?

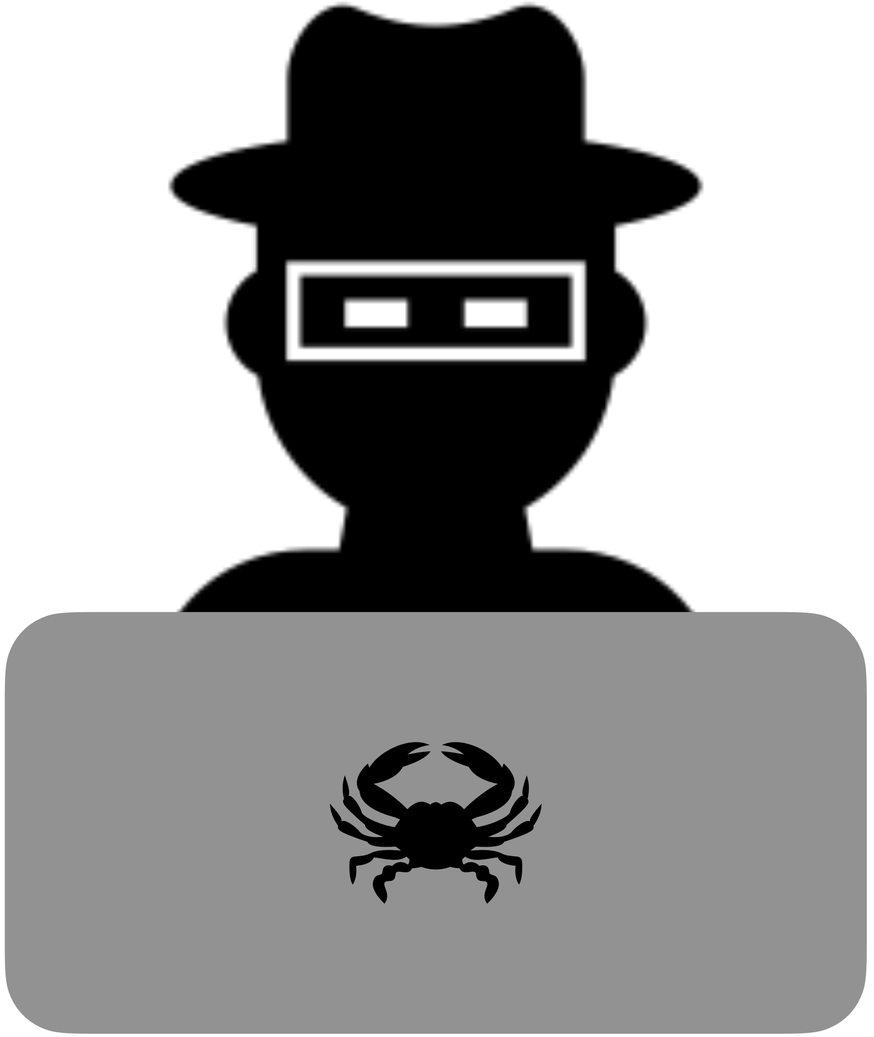
A skilled programmer who exploits vulnerabilities in a network of computer system in order to gain access to sensitive data or systems for illicit purposes.

Hacking is extremely illegal and carries serious sentencing if caught.
As a result, most hackers set their sights on really big targets.
Much like a bank robber, a hacker will try to commit one very big profile hack and then vanish without a trace.



Myth of the “Hacker”

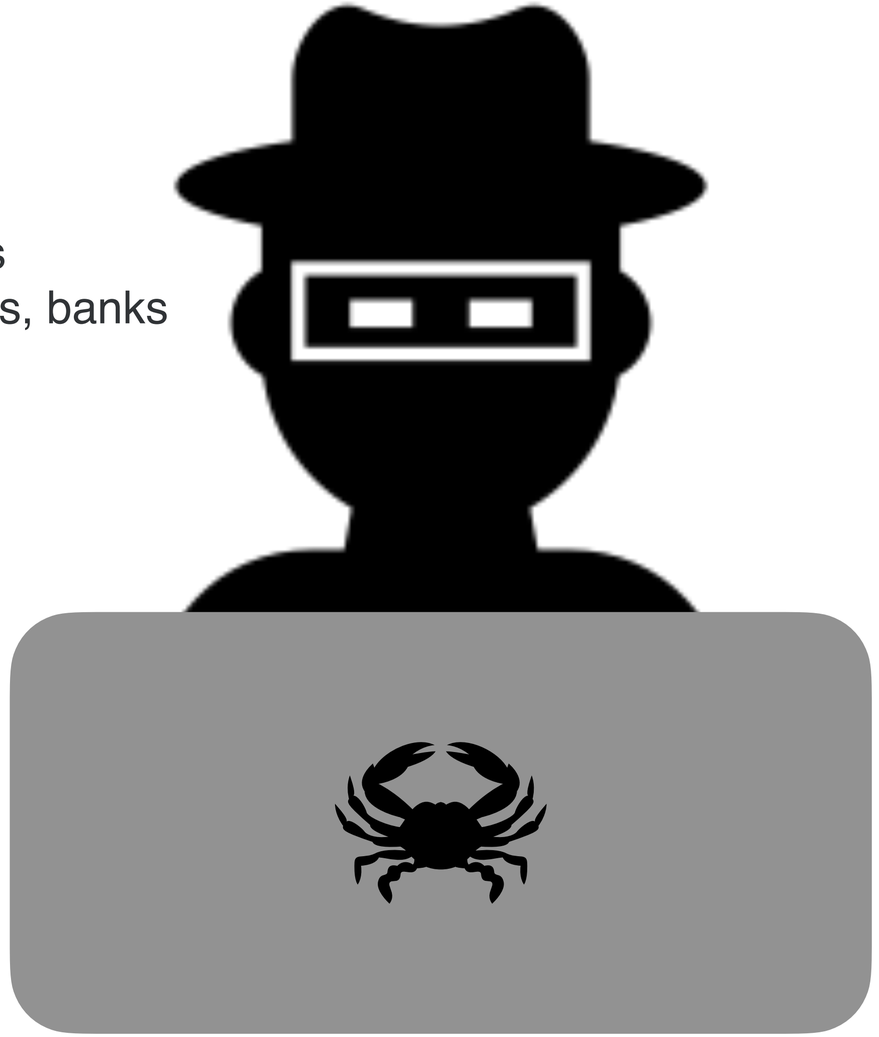
Types of Hackers



Myth of the “Hacker”

Types of Hackers

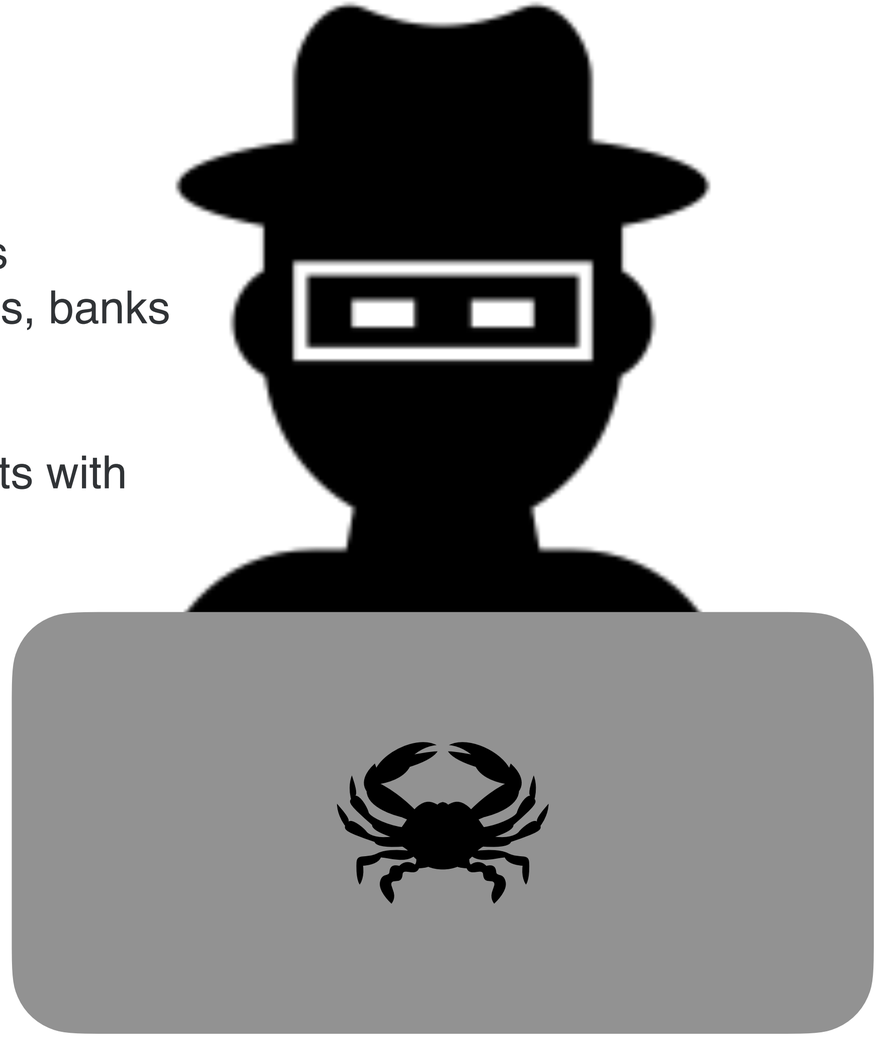
1. **The Good - White Hat** hackers are cyber security professionals. Their job is to hack the systems of the companies or organizations they work for. White Hat hackers often work for big tech companies, banks or governments. They hack the systems to identify flaws in the security which can be fixed.



Myth of the “Hacker”

Types of Hackers

1. **The Good - White Hat** hackers are cyber security professionals. Their job is to hack the systems of the companies or organizations they work for. White Hat hackers often work for big tech companies, banks or governments. They hack the systems to identify flaws in the security which can be fixed.
2. **The Bad - Black Hat** hackers are knowledgeable computer experts with criminal intentions. They attack computers and networks to gain access to systems where they do not have authorized entry.

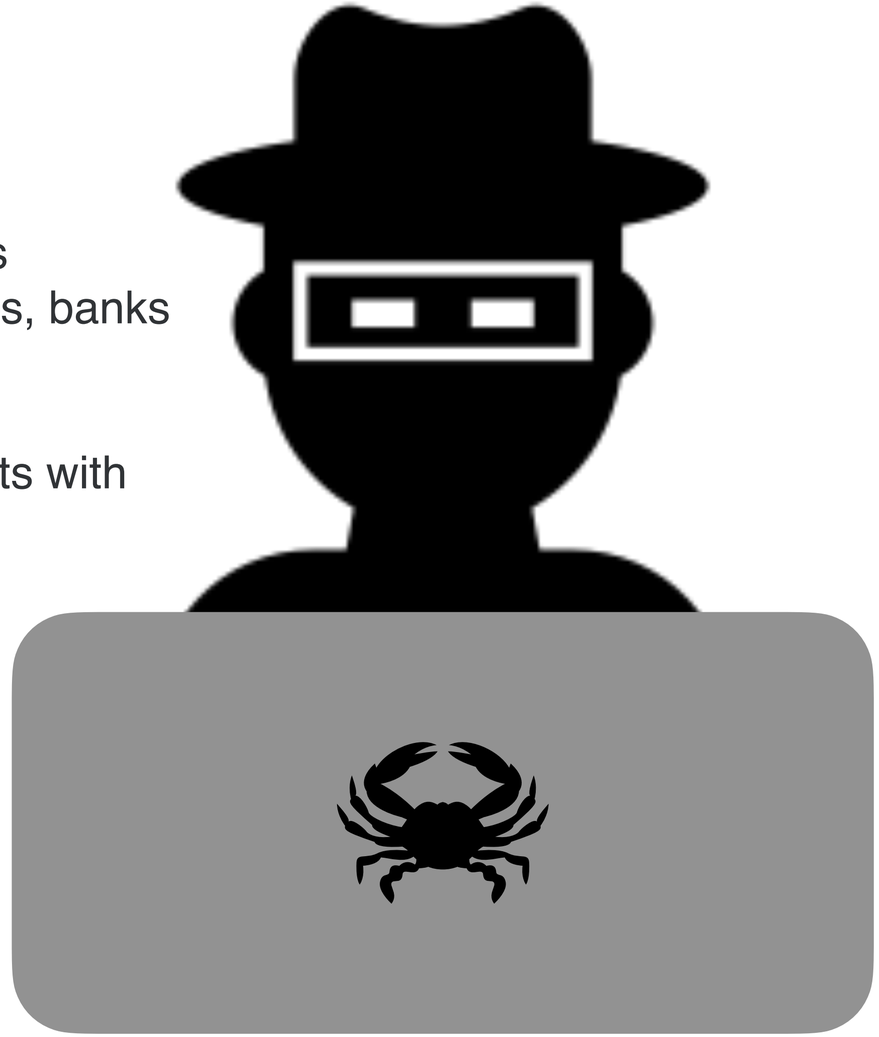


Myth of the “Hacker”

Types of Hackers

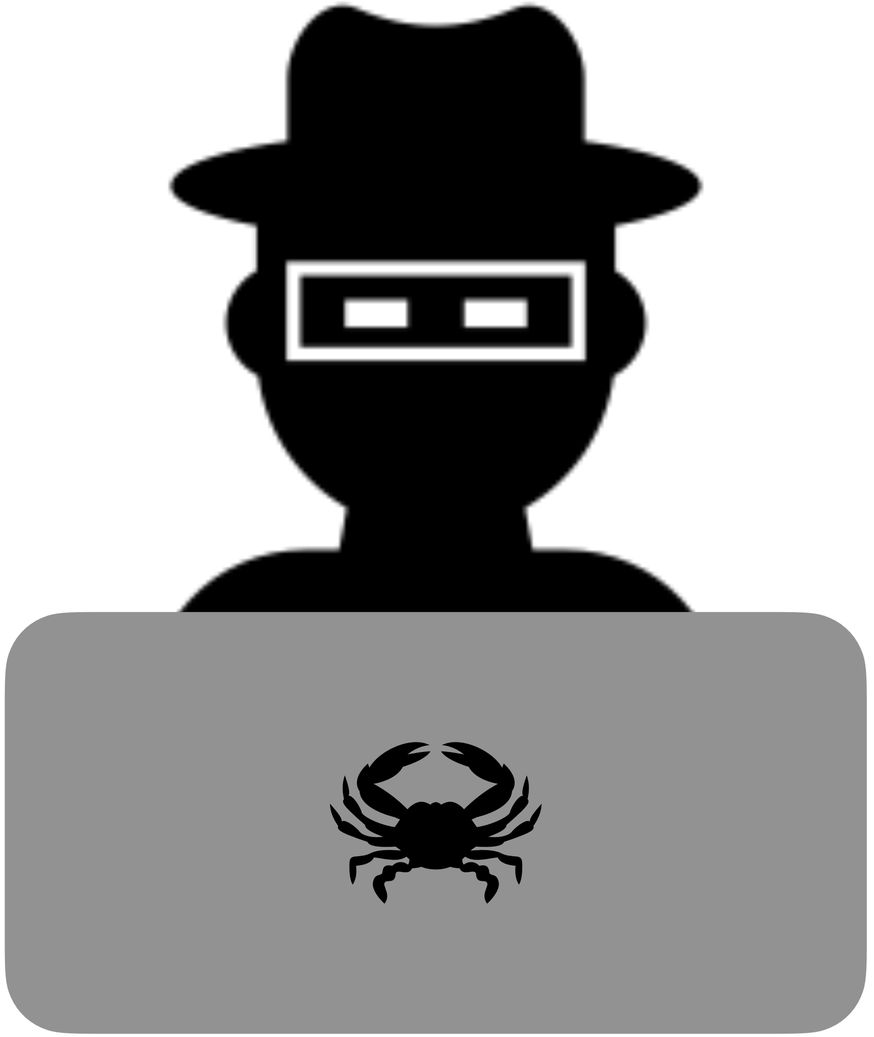
1. **The Good - White Hat** hackers are cyber security professionals. Their job is to hack the systems of the companies or organizations they work for. White Hat hackers often work for big tech companies, banks or governments. They hack the systems to identify flaws in the security which can be fixed.
2. **The Bad - Black Hat** hackers are knowledgeable computer experts with criminal intentions. They attack computers and networks to gain access to systems where they do not have authorized entry.
3. **The Stupid - Script Kiddies** are amateur hackers with little to no experience. They use tools or methods published by others online in the hopes of breaching vulnerable (often older and un-patched) systems using known vulnerabilities.

   Their actions are no less criminal than what a Black Hat hacker commits, but they are much worse at not getting caught.



Myth of the “Hacker”

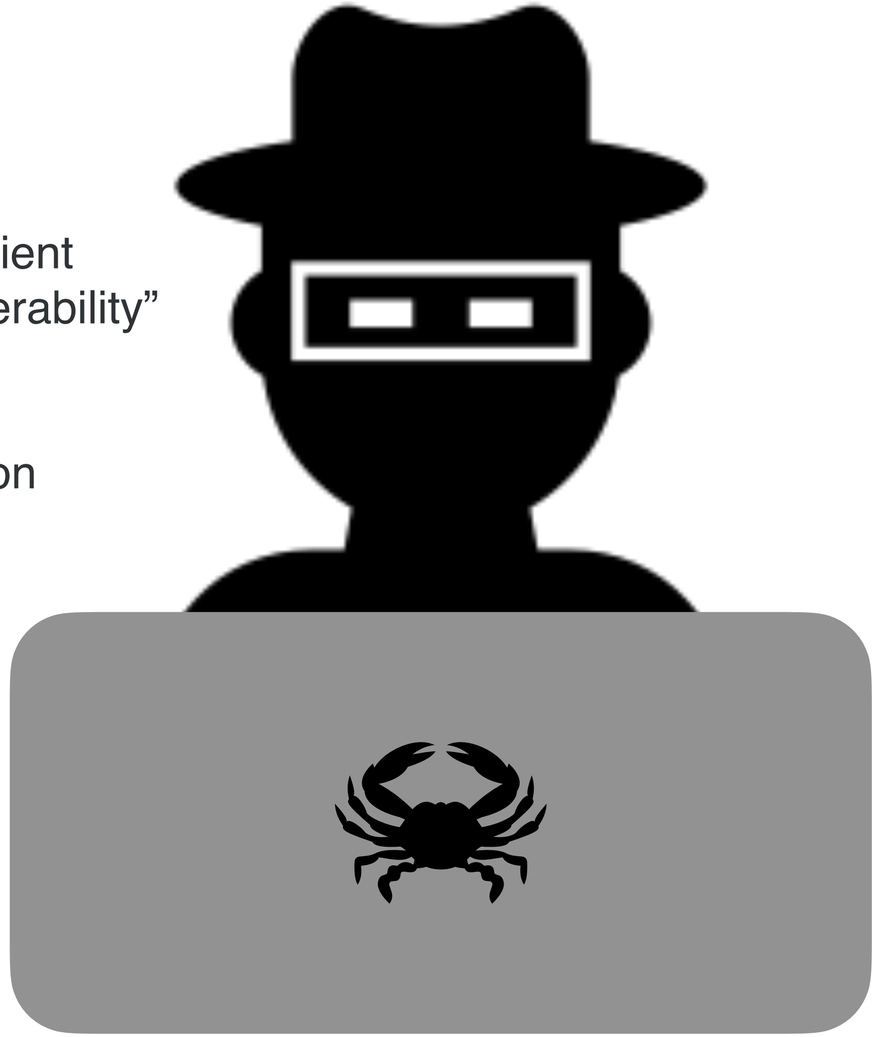
The Other Bad Actor



Myth of the “Hacker”

The Other Bad Actor

1. **The Scammer** - also known as a Phisher, Social Engineer, or Con Artist. The scammer is not someone who is necessarily proficient with technology but rather someone who attacks the “human vulnerability” in a system. Because a computer system is only as secure as the person using it, the scammer seeks to access the system not by defeating the software but by manipulating useful information out of its user such as username, password, or two-factor authentication codes.



Who gets hacked?

Common victims of hacking or “data breach”

Who gets hacked?

Common victims of hacking or “data breach”

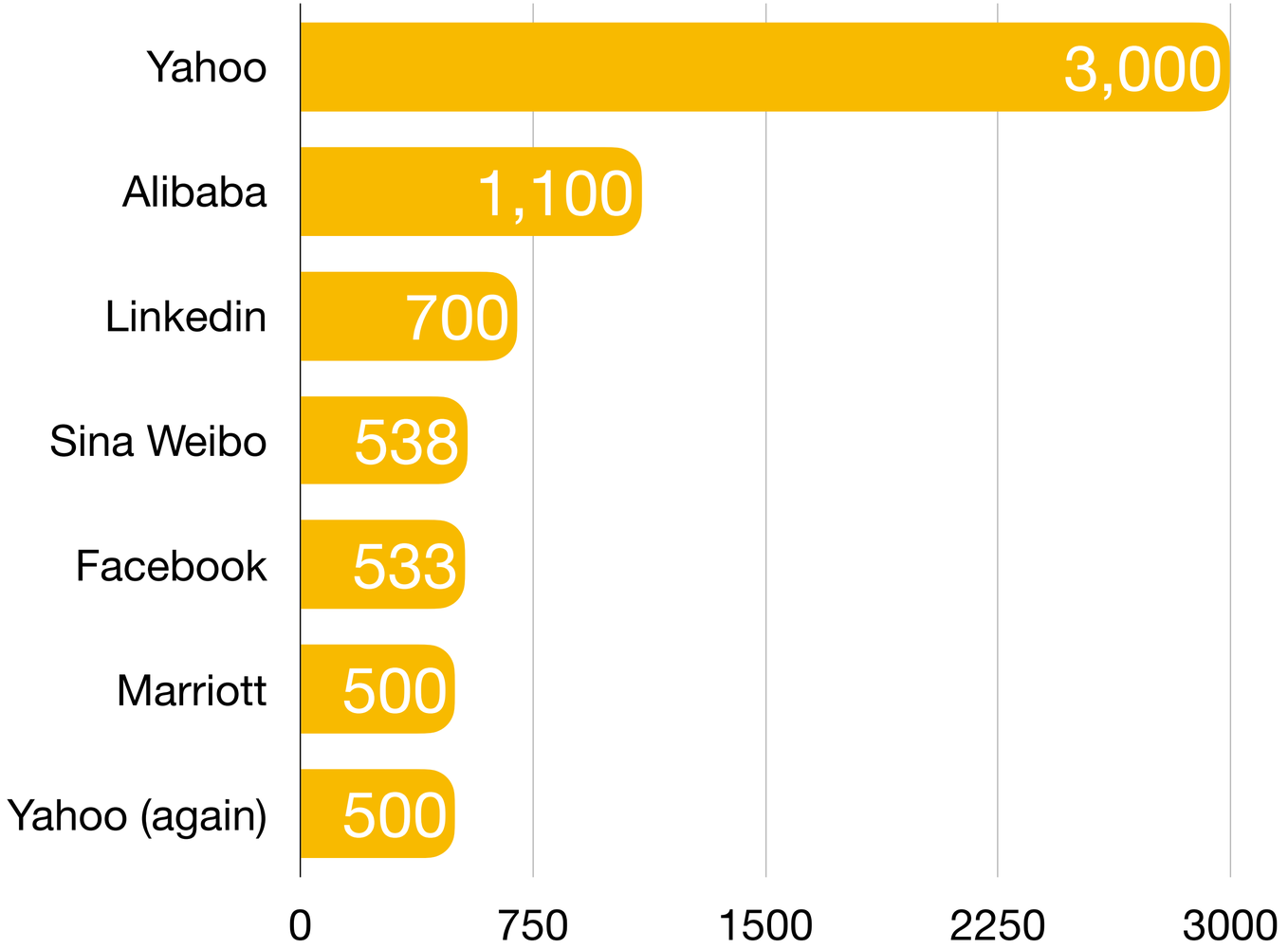
- Governments
- Companies
  - Email Providers
  - Cellphone Carriers
  - Credit Bureaus
  - Banks

Who gets hacked?

Who loses when companies get hacked?

YOU!

Biggest Data Breaches of all Time



AUGUST 19, 2021

NOTICE OF DATA BREACH:
Keeping you safe from cybersecurity threats.

What you need to know and how we're protecting you.

What you can do

Customers trust us with their private information and we safeguard it with the utmost concern. A recent cybersecurity incident put some of that data in harm's way, and we apologize for that. We take this very seriously, and we strive for transparency in the status of our investigation and what we're doing to help protect you.

What happened:

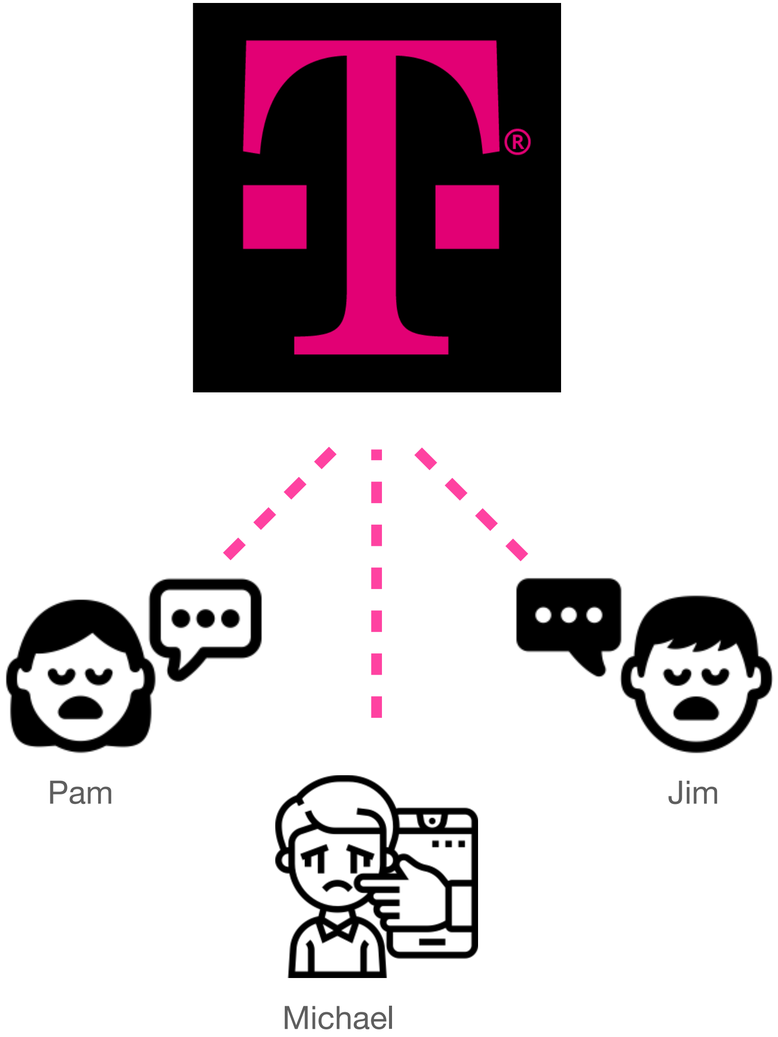
On August 17, 2021, T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information. The latest details about the affected data are available here.

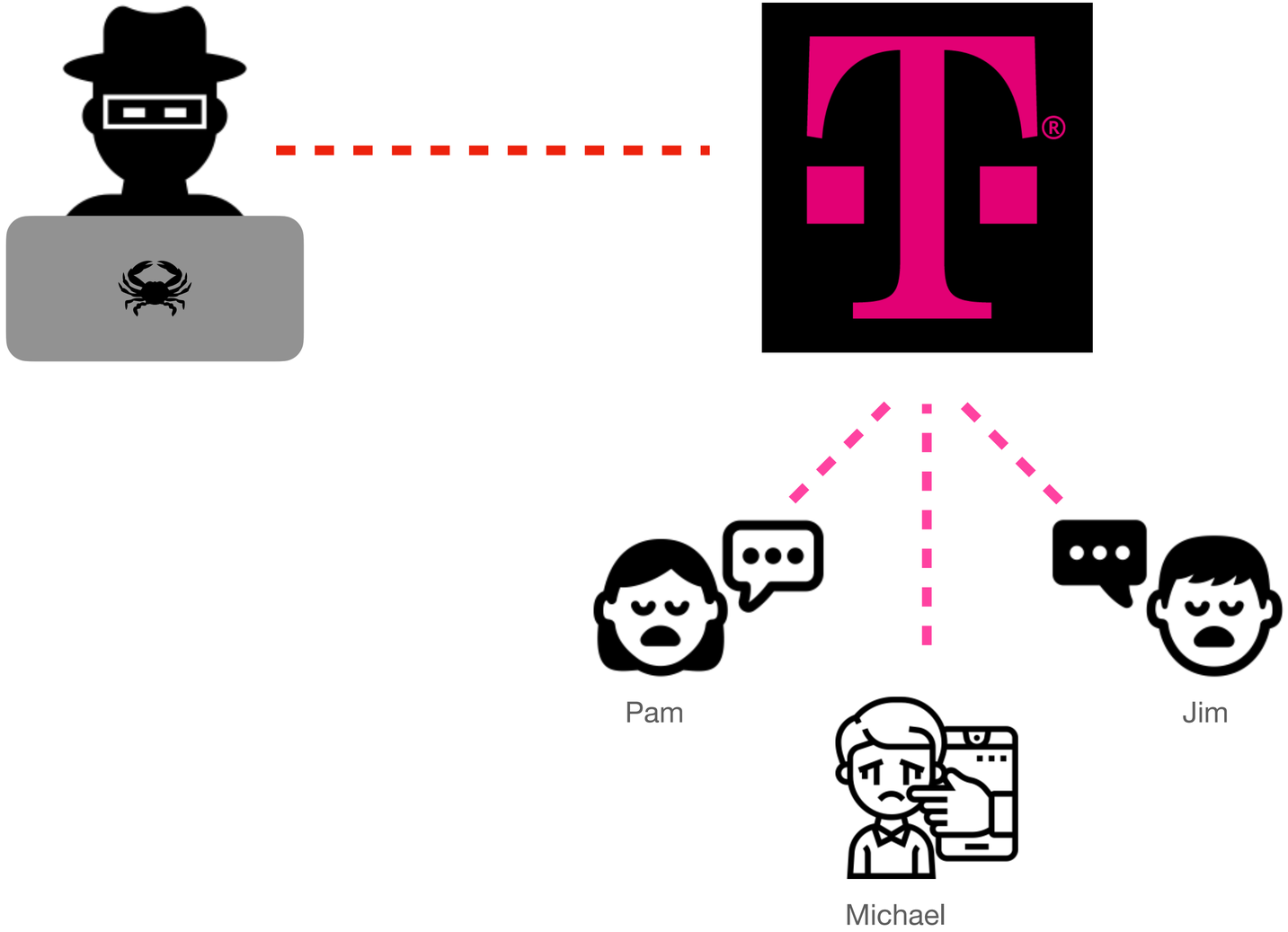
Information involved:

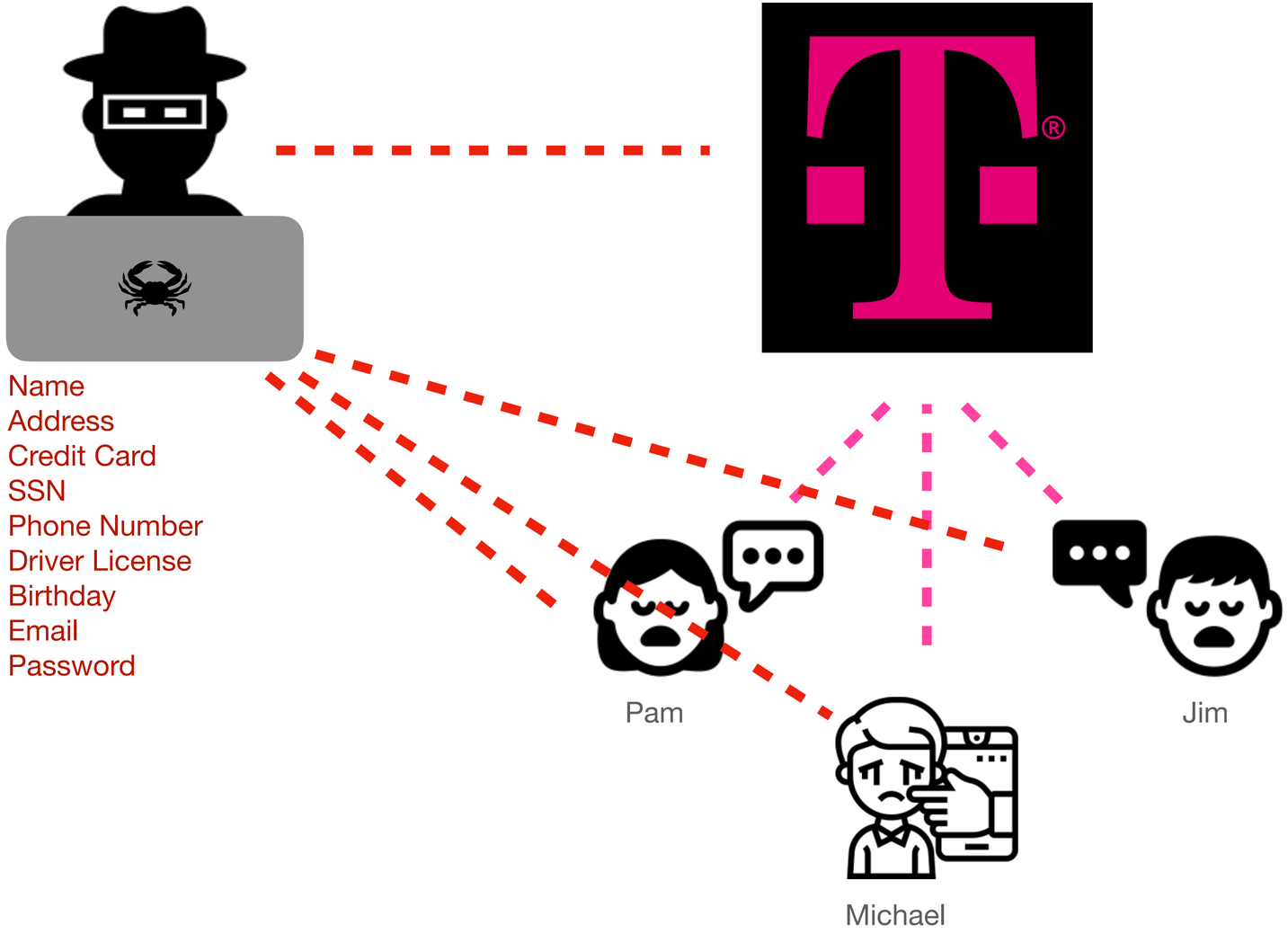
Our investigation is ongoing and this information may be updated. The exact personal information accessed varies by individual. We have determined that the types of impacted information include: names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s). **We have no indication that personal financial or payment information, credit or debit card information, account numbers, or account passwords were accessed.**

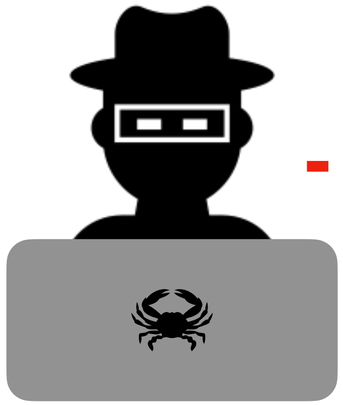
What we're doing:

We're relentlessly focused on taking care of our customers—that has not changed. We've been working around the clock to address this event and continue protecting you, which includes taking immediate steps to protect all individuals who may be at risk.

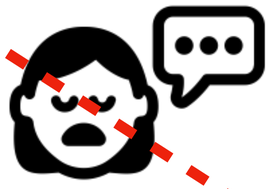

Pam
Jim
Michael


Pam
Jim
Michael


Name
Address
Credit Card
SSN
Phone Number
Driver License
Birthday
Email
Password
Pam
Jim
Michael



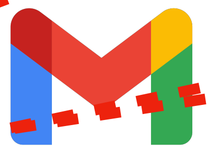
Name
Address
Credit Card
SSN
Phone Number
Driver License
Birthday
Email
Password

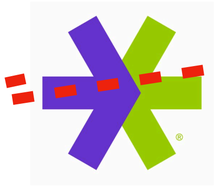


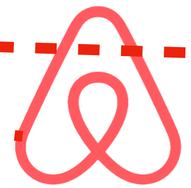
Pam

Jim

Michael







Digital Hygine

Security vs Convenience

Digital Hygine

Security vs Convenience

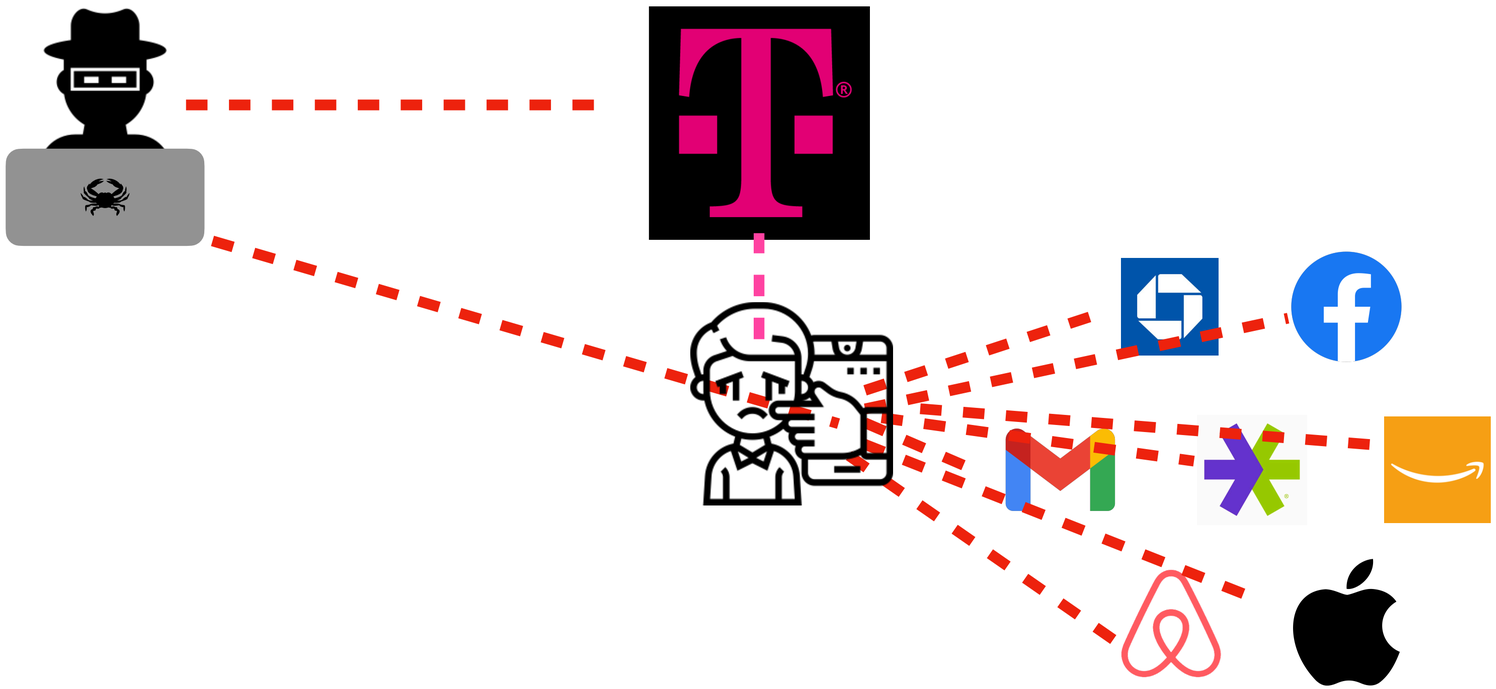
- Unique passwords for ALL accounts
- Password management tool
- Software Updates
- Use trusted WiFi only or stay on cellular
- Beware fake websites
- Never answer unknown numbers
- Don’t use “free” programs
- Only do business with reputable companies

Digital Hygine

Unique Passwords for ALL Accounts

- If you use the same information (especially password) for multiple services, a single breach can compromise all your accounts.
- It is inconvenient and even difficult to remember different passwords for multiple services. Variations on a theme can be helpful. Ex:

  3Tr@d3123456&
  Ch@s3123456&
  Tm0123456&
  F@c3123456&



Digital Hygine

Password Management Tool

- When memorizing passwords or making a pneumonic system proves too difficult, you can use tools like iCloud Keychain, Chrome, or 1Password to remember your account/password combinations

Digital Hygine

Software Updates

- Updating your OS and all your apps can be a pain. Who has time for that?
- Old software often contains vulnerabilities which can be exploited by bad actors who scan your system for known vulnerable software.
- New updates often contain security patches that improve your system’s defenses.

Digital Hygine

Software Updates

- “New software makes my machine run slow!”
- If you choose to skip updates because your computer or phone can’t handle the latest software, you are knowingly functioning at a risk. It’s time for an upgrade!

Digital Hygine

Use Trusted WiFi or Stay on Cellular

- When accessing the internet from an insecure network such as “Free WiFi” you might be exposing your browsing data (including passwords!) to whoever owns that network. Stay off unknown networks and if you are unsure just stay on cellular data.

Digital Hygine

Beware Fake Websites

- Look out for emails claiming to be a familiar company but use misspelled URLs (ex: app1e.com, g0ogle.com, aamazon.com, or web.ru/BofA)
- A legitimate company will NEVER ask you to click on a link and then put in your password.
- Use Bookmarks to trusted sites so you never miss-type and end up at an imposter site.

service@intl.paypal.com <service.epaiypal@outlook.com>

1/29/201

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Digital Hygine

Never Answer Unknown Numbers

- All phone calls are just junk these days
- Scammers trying to sell you car warranty, or steal your information
- If its important they will leave a message!

Digital Hygine

Don’t Use “Free” Programs

- This is more a tip for PC and Android.
- Free programs can often contain malware, adware, or outright viruses.
- Better to avoid anything that seems too good to be true!

Digital Hygiene

Only Do Business With Reputable Companies

- This one is tough. Even “good” companies get hacked. But picking who you do business with based on how actively supported they are, or if they a good business financially, or if they take stewardship of your data seriously.