

Let's talk  
Cybersecurity!





# What is cybersecurity?

the practice of protecting anything connected to the internet and mitigating the impact of any attacks or unauthorized access.

## What are we protecting?

- networks
- devices
- data

## Who are we protecting it from?

- unauthorized access
- criminal use



# Why should you care?



Your privacy is important.



Your data is important.



You are important.

Cyber criminals don't care who their victims are.  
They will attack anyone- businesses and individuals.



I have nothing to hide.



My family is not  
wealthy.

I'm not famous.

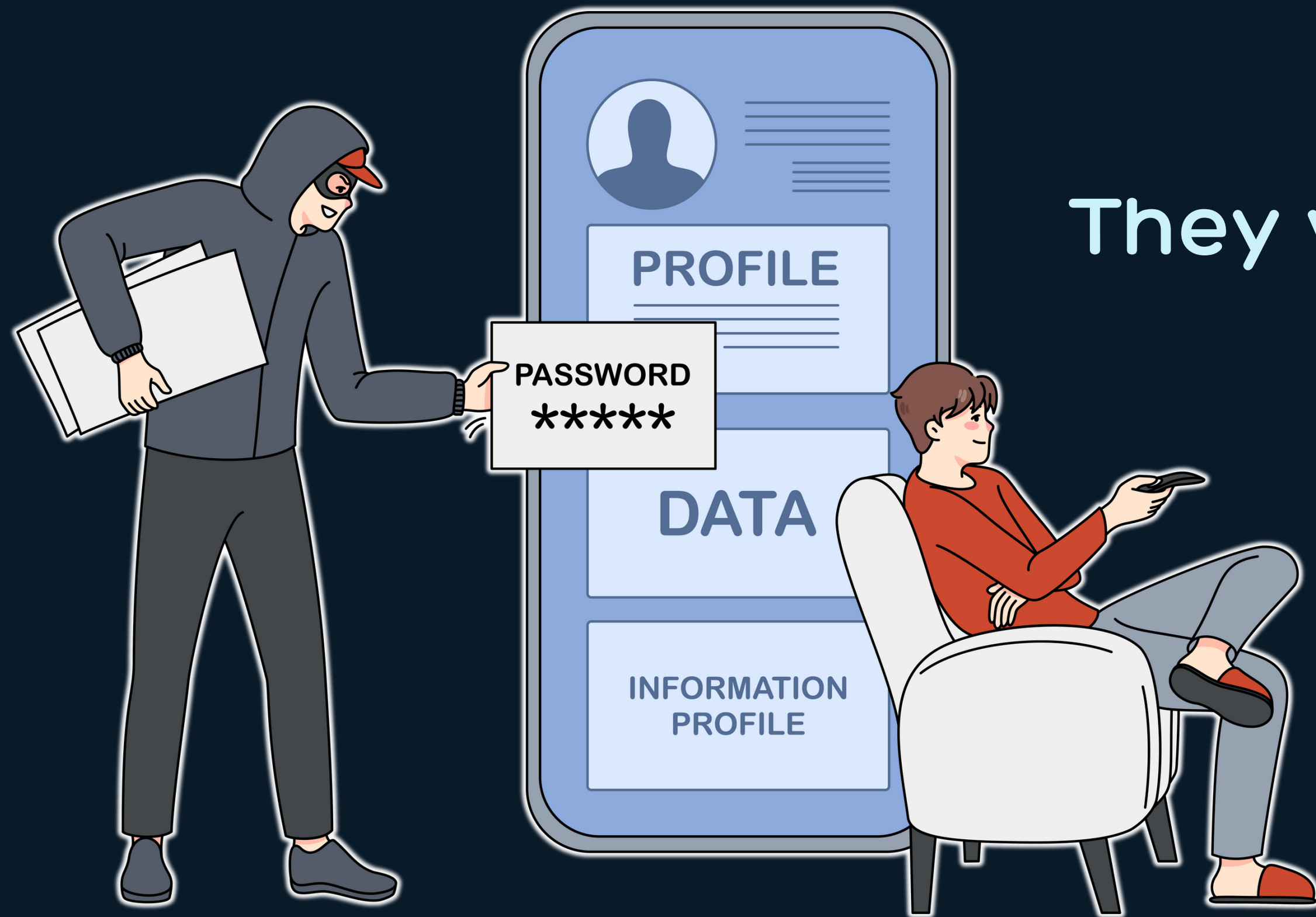


I don't have  
anything they  
want.

What can  
really happen  
anyway?



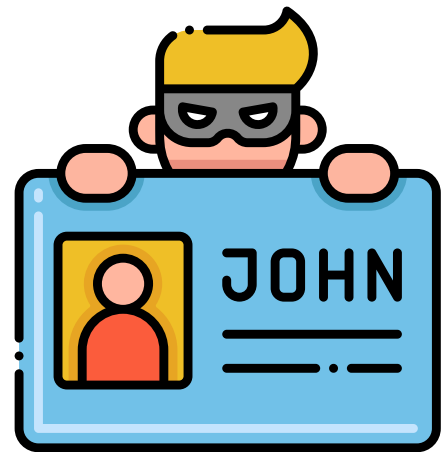
# What do cyber criminals want?



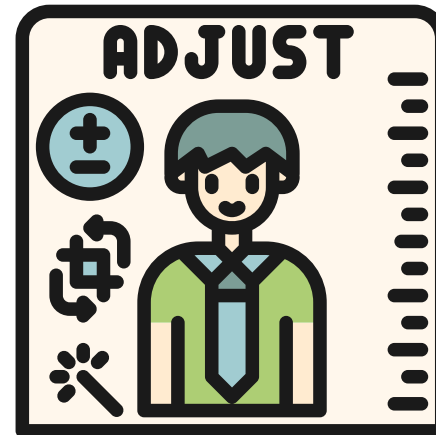
They want your data.

# How does a cyber attack impact your life?

It can have unexpected negative impacts on you that you may not have considered.



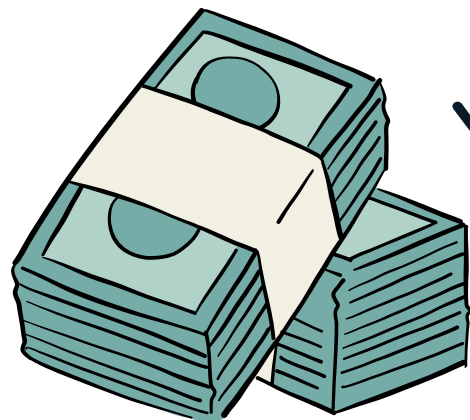
Your identity can be stolen.



Your photos can be taken, altered, & or used maliciously.



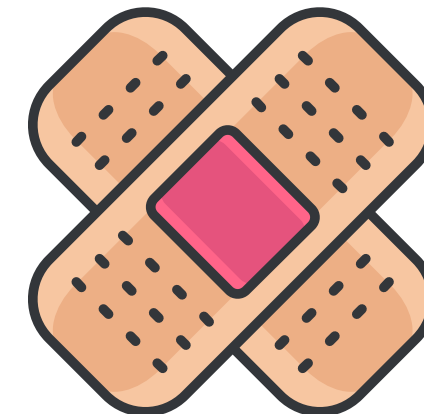
Your reputation can be harmed.



Your finances can be targeted.




Your personal sensitive info can be used.




You can be emotionally & or physically harmed.




# How do they do it?



Attachments  
or links in  
email or  
messages



Direct  
messages in  
social media  
apps



Public  
Wi-Fi




Exploiting  
vulnerabilities  
in software




Social  
Engineering




Applications -  
games, social  
media, camera  
apps, beauty apps,  
utility apps



QR Codes



Fake  
websites/  
Duplicates/  
Lookalikes



Job boards:  
fake job  
postings

There are many ways cyber criminals target their victims.



It's not a matter of IF  
an attack will happen.  
It's WHEN.





Cyber criminals have advantages we don't have:

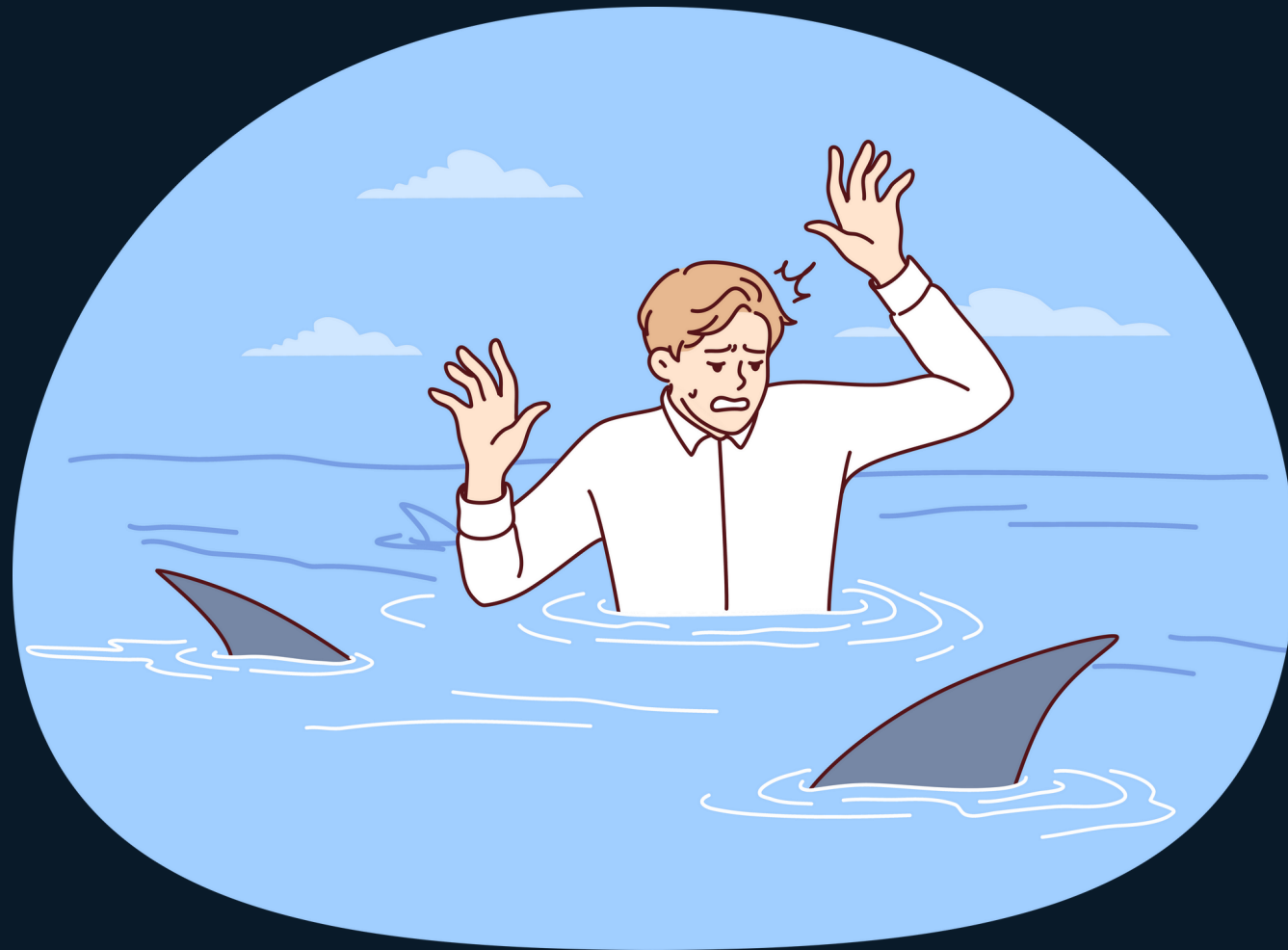
Time

Training

Resources



You may feel helpless.



As if there is nothing you can do.

But that's not true.



When we understand the risks,  
we can protect ourselves.

Follow these simple steps:



# How can I protect myself?

Be mindful. Be present. Pay attention.



Never share any private information about myself or intimate pictures.

Be careful about posting or sharing secrets with friends online.



Just because they look like a kid doesn't mean they are a kid.



Never share plans online - vacation, parties, etc.

Never give my real name and address online.





# How can I protect myself?



Back up your  
data frequently.  
Keep it offline.



By the way, never  
pickup a random usb  
you find. They may  
contain malware.

# How can I protect myself?



Keep devices,  
apps and  
browsers  
updated.

# How can I protect myself?

## Use antivirus/anti-malware





# How can I protect myself?



## Avoid Public Wi-Fi.

- NOT secure
- Use a virtual private network (VPN) if public Wi-Fi is a must.

## Avoid Public Chargers and Charging Stations

- NOT secure
- Ability to load malware on your device while it's charging.



# How can I protect myself?

## Passwords:

- Don't share passwords or account credentials.
- Enable and use multi-factor (MFA) authentication.
- Use a password manager versus saving your passwords in the browser.
- Change default passwords. (Routers, security cameras, etc)
- Use long, complex and unique passwords for EACH account.



# How can I protect myself?

Don't use one email for all your accounts.

Create email accounts specific to sensitive account needs: banking, government sites, etc.

Example: Don't use the same email for gaming, social media, and banking.





# Get Help.

When you see something wrong or something that makes you feel iffy, bad, or suspicious, please let an adult know.

It is not your fault. You won't get in trouble.

Parents, guardians, teachers and counselors, are here to help and support you.



# Parents and Guardians

Create a safe place for your child to talk to you about any problems they may face. Shaming & blaming doesn't fix anything.

Take advantage of parental controls.

Create rules for internet usage:

- Games, apps, social media sites must be reviewed by parents / guardians before use.
- Supervise online activities: periodically check their profiles & activities.
- Enforce time limits when necessary.

Be alert to changes in your child's behavior. Be calm and welcome your child to tell you what may be bothering them.

If you suspect any exploitation of your child, immediately report it "by calling 911, contacting the FBI at [tips.fbi.gov](https://tips.fbi.gov), or filing a report with the National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or [report.cybertip.org](https://report.cybertip.org)." Source: [justice.gov](https://justice.gov)



Thank you.

