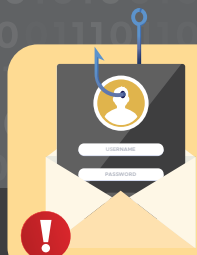


Cybersecurity Basics for the Every Day User



Protect Your Information



Personal Identifiable Information

- Name
- Phone Number
- Address
- Email
- Social Security Number
- Medical Information



Direct Access Information

- Financial Information
- Login Credentials

Attacker's Strategy



Create a sense of **Urgency**

Obligate a person to make a split second decision because they feel like they have no other options (example: Attacker saying "Call now otherwise you are authorizing this \$6,000 charge").



Target your **Emotions**

Put a person into a position to limit their logical thought, relying on emotions to make decisions (example: Attacker saying "If you do not make a payment, we will arrest you!").



Exploit your **Vulnerabilities**

For a device vulnerability, if a device is not up to date or a virus was downloaded, it is considered vulnerable. (example: attacker using a non-updated operating system to get into a person's computer).

For knowledge vulnerability, if a person is not a subject matter expert on a topic, they are vulnerable to relying on an attacker's "knowledge". (example: attacker suggesting "We are the Microsoft support team and can unlock").

To get to your Money

For an attacker it is all about the money, they will do what ever they can to get it.

Your Defense Strategy

✓ Do **DUST** frequently

Do...

- D** **Delete it:**
Remove anything not currently being used or stored.
- U** **Update it:**
Ensure that devices or programs are up to date.
- S** **Secure it:**
Back up important information and bolster defenses.
- T** **Track it:**
Know where devices are located and ensure a remote wipe of that device is a possibility.

Don't with **CATS** ✗

Don't...

- C** **Click it:**
Weigh the risk of every click and only click on trusted resources.
- A** **Acknowledge it:**
Avoid responding to untrusted sources, if it is important they will leave a message.
- T** **Trust it:**
If something seems suspicious, verify it is coming from the trusted source.
- S** **Share it:**
Keep information provided to a minimum, ensure what is being posted isn't enough to allow someone to impersonate.