

I'm Hacked, Now What?

SECURE YOUR DEVICES

- Disconnect all devices from the Internet - LAN (connected via a CAT or network cord), Cellular Data and Wi-Fi.
- Do not unplug any power sources if preserving evidence for law enforcement or insurance.
- Contact the bank.
- Remove any external devices connected to your device, such as, USB drives and printers.
- If there is an alternate device not involved in the compromise, use that device to log out of all financial accounts and any other shared accounts ie. Microsoft, Google, Facebook, etc.

PRESERVE IF THERE WAS A LOSS

- Contact law enforcement.
- Contact applicable insurance.
 - Ask your insurance company if they have a recommended malware mitigation solution that needs to be used to preserve any evidence should a claim need to be filed.
 - Ask permission to unplug your device before taking it to a professional.
- Stay in contact with the bank - timely cooperation is crucial.

CLEANSE & MONITOR YOUR DEVICES

- Contact a professional to scan the device (and any devices that were potentially connected to the infected device) for malware and viruses.
- Wipe the hard drive if necessary.
- Closely monitor credit and financial accounts - consider a credit freeze with all three credit reporting bureaus.