RANSOMWARE

You are the target.

THINGS TO REMEMBER:

What is it?

Ransomware is a type of **malware** that can...

- Cause apps, like your web browser, to stop working.
- Lock up your operating system.
- Encrypt your data and files so you cannot access them.

After infection, cybercriminals hold these resources for “ransom” and demand payment to unlock your resources, typically in the form of an online payment (i.e. Bitcoin, PayPal, etc.).

How do you get infected?

Ransomware often arrives in an email as a web link or attachment that downloads the malware when clicked.

YOU ARE THE TARGET

Anyone who uses a computer is a target. It’s possible to be infected with ransomware without even knowing it.

OHIO STATE IS A TARGET

Attackers target large companies and institutions because there are more resources to compromise, more damage to be done, more money to be made and higher stakes in general. Back up is more complex and restoration is more expensive, making large organizations more willing and likely to pay. Recently, another university was crippled with ransomware and opted to pay the ransom so they could return to normal operations.

PREVENTION

- Be aware of how to identify phishing emails so you can avoid being infected them.
- Don't click on links or open email attachments from sources you don't know.
- Only visit websites you know and trust.
- Be careful of documents asking you to enable features such as macros.
- Regularly back up your computer and test your backup to be sure it works.
- If you are unsure of a file, website or email contact your IT Service Desk.
- For more advanced safeguards, such as FIMs, whitelisting, or OS level checks, visit **go.osu.edu/ransomware**.

DETECTION

- Your computer displays warning messages that do not appear to be from your IT department.
- Files appear that you don't recognize, sometimes with unusual names.
- Your computer is locked or files are encrypted and cannot be opened.
- A message appears on your computer demanding you pay a fine or buy decryption software to unlock your computer.

CORRECTION

- If you think your computer or mobile device is infected:
  - Immediately alert your IT Service Desk.
  - Disconnect it from the network to avoid infecting other devices.
- Back up your computer regularly; the only safe way to remove ransomware is to restore your computer to factory settings. If you have backed up your files, you can then restore them without losing much data.