BUSINESS MALWARE 101

understanding malware & how to respond if your business is affected

What is malware?

Malware is any type of malicious software, installed without consent, designed to do damage or disable your business's computer system(s) or network.

TYPES OF MALWARE INCLUDE:

VIRUSES: malicious software attached to files and programs on infected websites, flash drives (USB), and emails activated by opening the infected application or file.

WORMS: malicious software that can transfer and copy itself from computer to computer.

TROJANS: malicious software that looks like a legitimate application or file, misleading a user to load and execute the malicious software onto their computer.

ROOTKITS: malicious software that enables an unauthorized user to gain control of a computer system without being noticed.

KEYLOGGERS: malicious software that records keystrokes made by a user in order to gain access to passwords and other personal/financial information.

RANSOMWARE: malicious software that blocks access to your organization's system or data until a sum of money is paid.

SPYWARE: malicious software that gathers data from your business's devices/systems to take control of its features.

ADWARE: software that displays advertisements and redirects your online search requests to advertising websites that collect marketing data about you.

Signs of malware can include slowed systems, new or unidentified icons, toolbar changes, and camera activation. Note that some malware can affect your computer or device with no immediate or noticeable symptoms.

What should you do if your business experiences a malware attack?

- Immediately remove infected computers or devices from your business network.
- Consider temporarily taking your network offline to stop the spread of malware.
- Isolate your backups immediately.
- Disable all shared drives that hold critical business information.
- Change all online account passwords and network passwords after removing the system from your network.
- Contact TechStak to get connected to vetted IT security providers.

Visit FraudSupport.org for more recovery resources.