CyberSecurity4biz.com

can your business survive without its data?

RANSOMWARE 101

As technology evolves, the prevalence of ransomware attacks is growing among businesses and consumers alike. It's important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code.

TIPS TO AVOID RANSOMWARE

KEEP A CLEAN MACHINE

Keep the software on all Internet-connected devices up to date. All critical software, including computer and mobile operating systems, security software and other frequently used programs and apps, should be running the most current versions. Turn on automatic updates in the security settings.

PROTECT YOUR SYSTEMS WITH SECURITY SOFTWARE

Install and keep security software (think of antivirus, antimalware & firewalls) current on all devices that are internet-connected.

GET TWO STEPS AHEAD

Turn on two-step authentication – also known as two-step verification or multi-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.

CyberSecurity4biz.com
can your business survive without its data?

RANSOMWARE 101

TIPS TO AVOID RANSOMWARE

BACK IT UP

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.

Use the 3-2-1 rule as a guide to backing up your data.

The rule is:

- keep at least three (3) copies of your data,
- and store two (2) backup copies on different storage media,
- with one (1) of them located offsite.

REPLACE THE PASSWORD WITH A PASSPHRASE

Get a passphrase, instead, which is a sentence that is at least 15 characters long. The longer the better. Focus on positive sentences or phrases that you like to think about and are easy to remember.

WHEN IN DOUBT, THROW IT OUT

Links in email, social media posts, texts, and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it. Definitely don't click on a link from a stranger. Employ an email scanning software that scans your email for suspicious emails.

RESTRICT USERS' PERMISSIONS TO INSTALL AND RUN SOFTWARE APPLICATIONS

This includes children and other family members on home devices, and employees on work devices.

CyberSecurity4biz.com
can your business survive without its data?

RANSOMWARE 101

SHOULD YOU PAY?

The FBI advises that you do not pay the ransom, as it only encourages and funds these cyber criminals.

Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files. However, NCSA does understand that this is a difficult decision to make, and you should consult with an IT expert or law enforcement before making a decision.

WHAT TO DO IF YOU EXPERIENCE RANSOMWARE

1. **Reach out to your IT expert,** IT department, or local law enforcement to help you respond if you are not an IT expert

2. **Identify** where your data backups are stored

3. **Report** the incident to FBI's Internet Crimes Complaint Center https://www.ic3.gov/default.aspx

RESOURCES

- **FBI:** Internet Crime Complaint Center
  https://www.ic3.gov/default.aspx
- **FBI:** Ransomware Overview
  https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- **FTC:** Ransomware Brochure & Quiz
  https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware
- **CISA:** Ransomware Overview
  https://www.us-cert.gov/Ransomware