Ransomware Attacks

What is it?

Ransomware is a type of malware that will prevent you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

How It's Done

The fraudster successfully installs ransomware onto a computer by sending an email attachment, ad, link,or website that's embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More nefarious versions can encrypt files and folders on local drives, attached drives, and even networked computers.

You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Avoid Being a Victim

- Be cautious and conscientious when it comes to clicking on links or downloading.
- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions automatically update and regularly run scans.
- Back up data regularly and ensure backups were complete.
- Secure the backups. Backups should not be connected to the computers/network they are backing up.
- Create a continuity plan in case your organization is the victim of an attack.

jbt Bank on a Smile.

jbt.bank

Member FDIC

EQUAL HOUSING LENDER