# Staying Safe Online

## Ransomware

TRUXTON TRUST
A PRIVATE BANK

### What is ransomware?

Ransomware is a type of malicious software designed by hackers to block a user's access to his or her computer until a ransom is paid. Once the malicious software is installed, the victim is no longer able to access data. At this point, the perpetrator demands ransom payment promising a way for the victim to regain access. The hackers will then demand a payment to allow the victim to access his or her data or they will represent themselves as a Microsoft (or other) support persons claiming to be able to clean up or fix the computer for a support charge. Ransomware began many years ago targeting individuals, but businesses and organizations are also at risk. Ransomware continues to evolve, but as long as you are prepared, you can stay one step ahead of it.

### How does it happen?

Ransomware is frequently delivered through emails. An email may contain an attachment or link, which appear legitimate, but carry malicious code that infiltrates the victim's computer. The malicious code typically either locks the victim's system or encrypts the victim's data, making it inaccessible.

### How do I protect myself or my organization?

Awareness is key. Educate and train yourself and all end users within your organization. Use reputable antivirus software and ensure it is up to date. Make sure your computers are regularly receiving updates and patches to their operating systems as well. The bulk of these updates are designed to address vulnerabilities in order to stay protected from the latest attack.

Exercise caution. Do not open attachments or click on links from email senders you do not know. Even if you recognize the name, check the actual email address. Verify that the email is legitimate by reaching out to the person via other means, such as a phone call, but not the number listed in the email. Back up everything valuable to you. If all of your data - documents, photos, and music - are copied to a separate hard drive or an online backup service, you diminish your risk.

### I've been infected, what now?

If you receive a ransomware note, disconnect from the network and shut down your computer. Do not pay the ransom. Paying a ransom does not guarantee access to your data. The FBI encourages individuals or organizations to contact a local FBI field office immediately to report a ransomware event and request assistance (www.fbi.gov/contact-us/field-offices). Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complaint Center (www.ic3.gov).

In the aftermath of an attack, make sure that your computer is free of malware. Use antivirus software to run a full scan of your computer or take the device to an IT professional for inspection. Change your passwords. Carefully review your financial statements each month for unauthorized activity or missing deposits. Early detection of fraudulent activity can be critical in limiting the damage. As always, if you have any questions or concerns, please do not hesitate to give us a call.