Staying Safe Online

Malicious Email

TRUXTON TRUST
A PRIVATE BANK

From unsuspecting individuals to major retail giants, cases of online fraud are rampant. The number of hackers, scammers, and cybercriminals continues to grow and the tactics to lure victims in are getting more creative…and harder to catch. The best way to keep you, your devices, or your business safe online is to stay educated and alert.

Malicious email is the most common type of online fraud. Often a malicious email looks nearly identical to a legitimate email. Read on to familiarize yourself with some common terms, tactics, and tips.

Spear Phishing

Spear phishing is a type of phishing scam where the perpetrator poses as a trusted, known, or legitimate source to get the victim to open an embedded link or attachment. The link may go to a website that also looks legitimate but is controlled by a hacker. The attachment may contain malicious software.

Keylogging

Keylogging involves a type of malicious software that provides the hacker with every keystroke made including account passwords and other personal information. This is often delivered as an email attachment or downloaded on a website.

Email Spoofing / Impersonation

Emailing spoofing is where a thief impersonates another person or company by "spoofing" or faking an email address, often a coworker, boss, or family member. The thief then asks for something, such as money, gift cards, or information. This request is often made with a sense of urgency or threat.

Ransomware

Ransomware is a type of malicious software designed by hackers to block access to your computer until a ransom is paid. This is often delivered as an email attachment or downloaded on a website.

- Avoid clicking suspicious links, downloading attachments, or responding to emails urging you to act quickly.
- Do not provide personal or financial information via email or on a website linked from an email.
- When in doubt, call the company or person who sent the email directly, but not from the information provided in the email.
- Keep all software, including antivirus, on your devices up to date. Perform operating system updates, which often contain security patches that try to stay ahead of potential attackers.

At Truxton Trust, we will never email you and ask you for your account, pin, or social security numbers. If you have any doubt, please do not hesitate to give us a call.

Call Us
615-515-1700

Visit Us
truxtontrust.com

Join Our Email List
Subscribe

Truxton Trust ■ 4525 Harding Road, Suite 300 ■ Nashville, TN ■ 37205