Be Wary Of Fake Invoice Phishing Attempts

The Federal Trade Commission reported a recent resurgence in phishing attempts. While phishing emails are not new, the FTC reports seeing an uptick of scams involving fake invoices from well-known tech companies.

How does this scam work?
A phishing attempt is when a scammer uses fraudulent emails, text messages or copycat websites to steal valuable personal information.

Criminals are sending out fake invoices from well-known tech companies in the latest version of this scam, according to the FTC. The scammers email victims phony invoices that say the recipients purchased music or apps from the tech company. The email then says to click on a link if the email recipient did not authorize the purchase. If the victim clicks on the link, scammers can get access to the computer and install ransomware. Or, if the phishing victim clicks the link and then enters personal information, the information can be stolen for the scammers to commit fraud or identity theft.

How can I protect myself?
Be cautious about clicking links or opening any attachments in email, especially if you were not expecting the email or something looks off.

Be suspicious if a business, government agency or organization asks you to click on a link that then asks for your username, password or other personal data. Instead, call the organization or type the web address directly into your web browser and sign in from there.

What if I’m a victim?
Always report all scams and fraud to your local law enforcement agency’s non-emergency number. If you believe someone is in danger, call 911. Report all scams and financial abuse to the state attorney general, and file a complaint with the Federal Trade Commission at ftc.gov/complaint.

Report phishing emails and texts by forwarding them to spam@uce.gov.