Cybercrimes

Ransomware

Malware is installed on your computer when you click on a link in an email. It holds your computer hostage by locking your screen or encrypting your files until you pay a specified amount of money for a key to unlock the system.

Phishing

The attacker will send an authentic-looking email, perhaps with a real organization's logo, attempting to steal passwords, financial or personal information, and introduce a virus. These emails are sent in bulk.

Spear phishing

This is a more targeted form of phishing. Emails appear to come from someone the recipient knows and trusts and can include a subject line or content tailored to the victim's work. Attackers may gain information from social media networks.

How to avoid them

• Always back up data so you won't have to pay the ransom.
• Add anti-virus software and pop-up blockers and check them manually for updates once a week.
• Don't click on links in emails. Instead, type in the URL manually to check its validity.
• Don't put individual email addresses on your website. Instead, set up a catch-all account such as contact@agency.com.
• Set your email to block all emails from outside the organization that have Microsoft office attachments. Your IT department can help.
• Don't call phone numbers listed in the emails, as those are generally fake. If an email comes from a company you already deal with, call the number you already have.
• Set up your email to read as plain text instead of html.
• Use a phishing filter. Many web browsers have them built in or offer them as plug-ins.

How to identify them

• Generic greetings or subject lines, such as "Bank Customer", "Friend", or "Subscriber"
• Requests for highly sensitive personal information
• Notes of urgency or deadlines
• URLs don't include the "S" in https://

What to do if you are a victim or suspect phishing

• Make your IT department aware immediately
• Contact local law enforcement, who will then contact the FBI
• Contact your bank, if they are involved

Top companies used in phishing emails

• Facebook and other social media
• Banks
• Logistics companies like UPS, FedEx, DHL and USPS