Most Dangerous Phishing Scams to Watch Out For

DECEPTIVE PHISHING

This is the most common type of phishing scam and it involves fraudsters impersonating reputable organizations to steal information or spread malware. These emails often convey a sense of urgency to scare victims into reacting quickly and doing exactly what the fraudsters want. The success of a deceptive phishing email hinges on how harmless and legitimate it looks. If it closely resembles a piece of official correspondence from a trustworthy entity, then people won't think twice about following its instructions.

SPEAR PHISHING

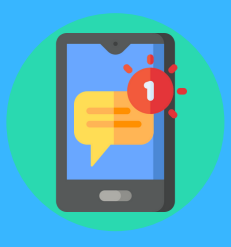
In this type of scam, fraudsters customize their emails with the target's name, company, and other information to make it seem like the correspondence is from a known or trusted sender. The goal of spear phishing is to trick victims into clicking on an unscrupulous link or downloading a malicious attachment to obtain their personal data. Given the amount of information needed to make a spear-phishing email as convincing as possible, fraudsters often lurk around social networking sites like LinkedIn where people's information is readily available.

CEO FRAUD

CEO fraud is a type of spear-phishing attack in which scammers impersonate a CEO or use a compromised email account of a high-ranking executive. They then trick an employee in accounting or HR into authorizing fraudulent wire transfers or disclosing confidential tax information. This type of scam works because executives are often not trained on their company's security policies.

VOICE PHISHING

Vishing (or voice phishing) takes place over the phone. A fraudster can set up a Voice over Internet Protocol phone system to mimic legitimate entities to coax victims into divulging sensitive information. So be extremely wary of calls asking you to verify your account information, provide your PIN, or answer your security questions. Elderly individuals as well as people with an aversion to technology are perhaps the most vulnerable targets, as they have little to no experience with these types of scams. A fraudster could call an elderly family member or relative and obtain your information from them.



SMISHING

Smishing leverages malicious text messages to trick victims into visiting malicious sites or handing over personal information. Smishing is particularly dangerous, as people are more inclined to trust a text message than an email. If you have any doubts, contact the organization directly (using their official communication channels) to verify if the messages you receive are authentic.

PHARMING

As users are becoming more aware of traditional phishing scams, some fraudsters are foregoing the idea of baiting their victims and are instead resorting to pharming. This involves installing malicious code on a computer or server and redirecting users to bogus sites without their knowledge or consent. Pharming doesn't require victims to click on any link for them to be taken to a fraudulent site — they are redirected there automatically. The fraudsters would then have immediate access to any information entered on the site.

Intelligent Technical Solutions

To protect your business from these dangerous types of phishing attacks, partner with ITS. Contact us today!