How to Avoid Phishing Scams

Protect Your Identity and Personal Data

Always Be Cautious Of...

Emails that ask for your sensitive personal information, such as your Social Security number or credit card information. Legitimate organizations will never send you unsolicited emails asking for sensitive information.

Emails that come from companies and government agencies where you did not initiate the action. These organizations will never initiate a dialogue with you via email and will never ask for personal information in such emails.

Emails that try to instill a sense of urgency, warn of some impending bad event (such as "your account is locked until you update payment information"), or that promise something that seems too good to be true. An email claiming you have won the lottery and need to enter personal details to claim your winnings is always fake. Attackers use these tactics to incite excitement or panic in potential victims, in the hopes of causing them to not think clearly and make poor decisions (such as giving them your personal information).

Emails that pressure you into bypassing established procedures and policies at work. They are most likely fraudulent.

Links in emails. While legitimate senders will send links in emails, links are also how attackers get victims to provide personal information and download malware. If you are unsure if an email is trustworthy, do not click any links in the email.

Attachments that accompany suspicious emails. Downloading attachments from a phishing email can and will often download malware onto your computer.

Poor spelling and/or bad grammar in emails. While even the most reputable sources will occasionally have spelling and grammar mistakes in emails, if an email is filled with spelling mistakes and poor grammar, it is a good sign that the email is not legitimate.

Poor layout and inconsistent formatting in an email as it is likely a phishing email. Companies often have dedicated employees that produce email messages, and it is unlikely that a reputable company would send any such emails to its customers.

Emails with a generic greeting, such as "Hello, Customer", because attackers use a generic message to send to as many people as possible. However, spear phishing (phishing specifically targeting a specific group or person) attacks will often use your name. So, just because an email does specifically address you, doesn't mean you should let your guard down.

How to Avoid Phishing Scams

Protect Your Identity and Personal Data

What You Should Do to Protect Yourself

Hover over any links in the email to see where the link is actually going to take you, being very careful not to click the link. (If you are on a desktop or laptop when receiving a suspected phishing email)

> If a link looks like it goes to www.ny.gov, it doesn't necessarily mean that's where it is going. When you hover over the link, a box will appear, often in the bottom of the screen, that shows where the link points to. If the address in this box is different than what the link says, there's a good chance that the email is malicious. Be aware it may be the difference of a single letter.

Check the domain name that the email is coming from. Watch out for emails with misleading domain names in the links. For example, account.microsoft.com is a legitimate subdomain of microsoft.com, which is a legitimate and trusted website.

> However, account.microsoft.harrythehacker.com is not legitimate. Even though the link says account.microsoft in it, notice how the right-hand side of the link is harrythehacker.com and not microsoft.com. This means that the link is going to a site controlled by Harry the Hacker and NOT Microsoft. Attackers often use this trick and others like it to make victims think they are going to a trusted website.

Call the sender of the email to make sure it is really from them. Attackers can make emails look like they are coming from friends, family, or colleagues. If a message you received from a friend or colleague sounds "off" or uses grammar and wording that doesn't sound like that person, give them a call.

> Along the same lines, if you are suspicious about an email received from an organization, contact them directly to confirm if the email is legitimate.

Always keep your guard up, even with emails that appear to be from trusted sources. Attackers can easily make their emails appear to come from reputable sources, such as Microsoft.com or even a government website such as ny.gov

integrated systems

Important Phishing Key Words to Know

Hover: Alternatively referred to as mouseover or mouse hover, hover describes the act of moving a mouse cursor over a clickable object, but not actually clicking the left or right mouse button.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Phishing: The fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, credit card numbers, or other sensitive details by impersonating oneself as a trustworthy entity in a digital communication, such as an email.

Domain Name: A website's equivalent of a physical address. In the same way that a GPS needs a street address or a zipcode to provide directions, a web browser needs a domain name to direct you to a website.

A domain name takes the form of two main elements. For example, the domain name Facebook.com consists of the website's name (Facebook) and the domain name extension (.com). When a company (or a person) purchases a domain name, they're able to specify which server the domain name points to.

Subdomain: A subdomain is an additional part to a main domain name, located at the first portion of a link to the website. Subdomains are created to organize and navigate to different sections of a website.