

What is Phishing?

Phishing is essentially an online con game, and phishers are nothing more than tech-savvy con artists and identity thieves. They use spam, malicious websites, email messages, instant messages and even phone calls to trick people into divulging sensitive information.

Since phishing scams are designed to appear as if they come from reliable sources, it is smart to know the difference between real and fraudulent messages and how to spot some of the clues that a message may be a scam. Read below about the common types of phishing scams and tips to help you avoid falling into their trap.

1: Email Phishing Scams

Phishers commonly use real company logos and spoofed email addresses to make their communication seem legitimate. The message entices the recipient to provide information that could be used for identity theft or online financial theft. A phishing message typically includes a link to a fake website or attachment that is designed to mimic the site or document of a legitimate business.

2: Vishing Scams

Vishing is the voice version of email phishing. It is a phone scam in which individuals are tricked or scared into handing over personal information to scammers.

3: Tech Support Call Scams

Tech support calls are when a scammer calls a potential victim claiming to be from a reputable security company. They claim to have found malware on the victim's computer and offer a solution by getting the user to install a type of remote desktop software. This allows the attacker access to the computer and install real malware. These scammers will often ask for a fee to "fix" the issue.

4: Pop-up Warning Scams

Pop-ups occur when someone is browsing the internet and sees a small graphic or ad appear on their screen. Malicious pop-ups can be terribly intrusive, making it difficult for the user to close the pop-up window. These pop-ups may display a message stating that the computer is infected with malware and offer a phone number for help with removing the malware.

5: Fake Search Results Scams

Fraudulent companies frequently use paid search ads for their "support services" and can appear at the top of a search results page. These results, which can look like the real thing, can promise offers that seem too good to be true in hopes of luring in a victim. Unfortunately, when you click on the ad, malware may begin to download to your device, compromising the security of your information and adding to your computer woes.

Tips to Avoid Phishing Scams

Nobody wants to fall prey to a phishing scam. There's a good reason that such scams will continue, though: They are successful enough for cybercriminals to make massive profits. Phishing scams have been around practically since the inception of the Internet, and they will not go away any time soon. Fortunately, there are ways to avoid becoming a victim yourself. Here are 10 basic guidelines in keeping yourself safe.

01 Keep Informed About Phishing Techniques

New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one.

02 Think before You Click

It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with "Dear Customer" so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.

- Never click on links, download files or open attachments in emails or social media.
- Pay close particular close attention to shortened links, especially on social media.
- Does the email look suspicious? Read it again.
- Be wary of threats and urgent deadlines.

03 Install an Anti-Phishing Toolbar

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

04 Verify a Site's Security

It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar. Check for the site's security certificate as well.

05 Check Your Online Accounts Regularly

If you don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

06 Keep Your Operating System and Web Browser Up to Date

Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.

- Never allow remote access to your computer

07 Use Firewalls

High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

08 Be Wary of Pop-Ups

Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don't click on the "cancel" button; such buttons often lead to phishing sites. Instead, click the small "x" in the upper corner of the window.

09 Never Give Out Personal Information

As a general rule, you should never share personal or financially sensitive information over the Internet. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with "https".

- Never give personal information over the phone. Hang up, look for the number of the company on their website, and call them directly to make sure it was a legitimate call and request.
- Never call the number the caller provides. When looking up the company website, make sure it is legitimate. Fake websites often contain misspellings and other telltale signs

10 Use Anti-Virus Software

There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date. New definitions are added all the time because new scams are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks. Antivirus software scans every file which comes through the Internet to your computer. It helps to prevent damage to your system. You don't have to live in fear of phishing scams. By keeping the preceding tips in mind, you should be able to enjoy a worry-free online experience.

What To Do If You've Been Scammed or Your Personal Information Has Been Compromised

- Change your passwords. Your computer, financial institutions, and any other password-protected websites that you visit should be updated.
- Run a Full System Scan for viruses on your computer.
- Contact your bank to report that you may have been the victim of fraud
- You can also place a fraud alert with one or all of the three credit bureaus
 - Experian: 1-888-397-3742
 - TransUnion: 1-800-916-8800
 - Equifax: 1-800-685-1111

To sign-up for scam alerts, get information on the latest scams, and learn more about how to prevent yourself from becoming a victim visit:

<https://www.consumer.ftc.gov/features/scam-alerts>