

10 Ways to Protect Yourself Against Phishing Attacks



We can't overestimate the importance of education when it comes to improving our awareness of phishing and other digital security threats. That is why I discussed some tips to help users spot a phishing scam in a recent article. We also mention some of the best anti phishing solutions.

Knowing what to look out for in a phishing attack is important. But that's only half the battle. Users also need to take concrete steps to deter phishers and keep their information safe.



Acknowledging that fact, here are 10 ways you can protect you and your computer against a successful phish.

10 Cyber Safety Tips

1. Don't Panic

Phishers commonly incorporate threats and a sense of urgency into their attack emails. There's a purpose for doing so. As fellow human beings, they know that we make some of our worst decisions when we're panicked and not thinking clearly. We might even allow ourselves to click on a suspicious link or forfeit some of our sensitive personal information.

With that being said, try to remain calm if you receive a threatening or otherwise alarming email. That way you can make informed decisions and avoid falling victim to a phishing scam.

1. Enter Sensitive Information Only on Secure Websites

A majority of phishing attacks request that users send over their personal information either by email or by entering it into a fake login form on a malicious website. To protect against this tactic, try to submit your personal information only on secure websites. In the very least, those websites should have a written privacy policy outlining how they will use/store your personal information. They might also have a signed certificate for HTTPS, which will help protect the privacy and integrity of any data you exchange with them.

1. Familiarize Yourself with a Website's Privacy Policy Before Signing Up

Just because a website uses HTTPS doesn't necessarily mean you should share your personal information with it. Some websites sell your email address and other contact information to third-parties. Those buyers might in turn sell your data to non-reputable individuals who could save your information and target you in future phishing attacks.

Be on the safe side. Before sharing your information with a website, review the site's privacy policy and make sure you agree with its terms and conditions.

1. Hover Over Suspicious URLs Before Clicking on Them

Attackers like to trick their targets into clicking on a seemingly benign URL that in actuality leads to a malicious domain. Fortunately, users can easily expose that ruse by hovering over a suspect URL. Does it link to where its text says it does? If not, you can be sure the URL's true destination is malicious in nature.

1. Exercise Caution Around Shortened Links

Not all URLs give up their actual link locations when you hover over them. Take shortened URLs, for example. Services such as bit.ly and tinyurl might help reduce URL size and track links. However, a URL that has been shortened reveals no information about its actual destination. It could lead anywhere, even to phishing pages.

Legitimate organizations are aware of this skepticism, so they generally don't incorporate shortened links in any business correspondence. As a result, if you receive an email containing shortened links from an organization, think twice before clicking on them.

1. Install an Anti-Virus Solution on Your Computer

While many phishing attacks extract user credentials via a fake log-in form, others install malware onto a user's computer and leverage keyloggers to collect usernames, passwords, and other sensitive information.

To help protect against a malware infection, install an anti phishing software solution onto your computer and make sure it is up-to-date so that it can detect the latest threats.

1. Implement Vendor Updates as Soon as They Become Available

One of the ways phishers deliver malware to a user's computer is via exploit kits, or software kits that exploit vulnerabilities in popular software to infect users with malicious programs. Some of the most well-known exploit kits, such as Angler, Neutrino, and Magnitude, commonly drop ransomware onto vulnerable computers. Those crypto-malware variants encrypt users' files and demand hundreds if not thousands of dollars in ransom for the decryption key.

Exploit kits are most effective at targeting computers with known software vulnerabilities. Don't open yourself to attack by leaving these types of issues unpatched! Try to update your system as soon as a vendor releases a security upgrade or software patch.

1. Enable Content Only on Documents from Trusted Sources

Another way phishers like to infect users with malware is via malicious email attachments. In particular, fraudsters like to trick users into opening a seemingly innocent Word document that asks them to enable content. Unfortunately, that "enable content" button is in these types of emails a malicious iframe. When clicked, it initiates a downloader that passes malware onto the user's computer.

Users need to approach the "enable content" button in Office documents carefully. Only when they know the document originated from a trusted source should they click the "enable content" button. Even then, it's a good idea to contact the sender beforehand and confirm they sent you a document with some content disabled.

1. Contact the Sender

Contacting the sender isn't just a good way to protect against malicious content (macros). It's a good way to protect against all types of phishing attacks.

If you receive a suspicious email from a friend, family member, business, or other trusted source that seems suspicious or out of character, contact them and confirm whether they actually sent you the message. They might say they did, or they could reveal they were recently hacked.

1. If in Doubt, Delete the Email

Some suspicious emails don't come with any usable contact information about the sender. If that's the case, try to research the sender and see if you can find out any information about them. If you are unable to do so, it's better to just delete the email and not take any chances with your computer's security.

Conclusion

By studying the above-mentioned tips, you now know how to protect yourself against a variety of phishing attacks.

Unfortunately, phishing scams are always evolving and incorporating new techniques to target unsuspecting users. It is therefore important that you and your entire company conduct ongoing anti-phishing exercises to stay on top of the latest phishing attacks. Also have a look at the best anti-phishing software solutions for your own computer.

Modern organizations are dependent on their digital network to survive and operate in today's business world. The Metacompliance solution assists with the challenge of Cyber Security Awareness, Simulated Phishing, Incident Management, Policy Management and Knowledge Assessment.

Metacompliance has developed a solution to help defend the company by improving user awareness of cyber security and compliance risks.

Simulated Phishing, Incident Management, Policy Management and Knowledge Assessment.

Metacompliance, a provider of policy management software and user awareness training, offers many off-the-shelf solutions that allow companies to streamline their employee security awareness

training. Those products include MetaPhish is a, a software solution specifically designed to conduct ongoing phishing simulations to help increase your employees' sensitivity to these fraudulent emails.

To learn more about MetaPhish and how you can better protect your organization against phishing attacks, please click [here](#).