



10 Ways 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:

1. 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. For IT administrators, ongoing [security awareness training](#) and [simulated phishing](#) for all users is highly recommended in keeping security top of mind throughout the organization.

2. 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. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? 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.

3. 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.

4. 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. If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishing webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by cybercriminals.

5. 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.

6. Keep Your 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.

7. 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.

8. 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.

9. Never Give Out Personal Information – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. 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".

10. Use Antivirus 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.

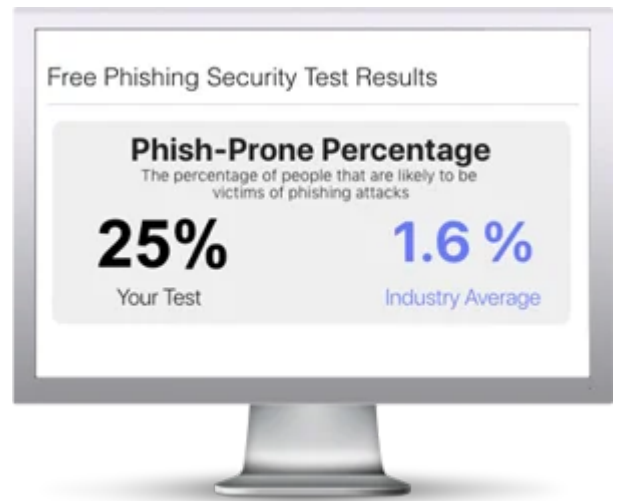
Remember there is no single fool-proof way to avoid phishing attacks,

Free **Phishing Security Test**

Would your users fall for convincing phishing attacks? Take the first step now and find out before bad actors do. Plus, see how you stack up against your peers with phishing Industry Benchmarks. The Phish-prone percentage is usually higher than you expect and is great ammo to get budget.

Here's how it works:

- Immediately start your test for up to 100 users (no need to talk to anyone)
- Select from 20+ languages and customize the phishing test template based on your environment
- Choose the landing page your users see after they click
- Show users which red flags they missed, or a 404 page
- Get a PDF emailed to you in 24 hours with your Phish-prone % and charts to share with management
- See how your organization compares to others in your industry



Go Phishing Now!

PS: Don't like to click on redirected buttons? Cut & Paste this link in your browser:

<https://www.phishing.org/phishing-security-test>

Related Pages: [Phishing Techniques](#), [Common Phishing Scams](#), [Report Phishing](#)

