**HOW TO AVOID SPAM AND PHISHING MAILS**

**5 Best Practices to Combat Email Spam**

Currently, there is no way to completely stop spam. The good news, however, is that individuals can take proactive steps to limit the number of incoming spam emails to save time, frustrations and money.

**1. Keep Your Email Address More Private**

To avoid email address harvesting practices, it's important to not post (in text) your email address in public Internet chat rooms, on any Web site, newsgroup, guestbook or blogs to which you post. If you find you need to post an email address, try typing your address in a graphics program and using an image of your address in a signature file or attachment. Or, you can also replace common characters (such as the @ or .) with spaces or spelling. For example, writing your address as  
"webmaster — at— webopedia —dot— com" is one way to display your e-mail address so humans can understand it, but software or script harvesters cannot grab it and add it to a spam list.

You can also consider encoding your email address by using its equivalent decimal entity. To people viewing the address in a browser, it appears as normal text. The code, however, consists of character entities and unreadable to many harvesting scripts.

If you plan to participate in online forums or newsgroups, or you plan to join different mailing lists, you can always register for a free online Web mail account. This will help filter the bulk of spam from publicly posting your e-mail address to one email account that is not used for family, friends or work-related communications. It doesn't mean your other accounts won't get spam, but it will help you time-wise by enabling your other account to have less spam build-up.

**2. Choose More Complex Email Addresses**

Some spammers basically attack mail servers and use a method called a dictionary attack to get their junk mail sent out. Basically, the spam is sent to every combination of letters and common names at an ISP. In this scenario, spam is more likely to get through to a common, short email address like "mary @insertdomainname.com" than it would "marywashinger @insertdomainname.com".

**3. Don't Click Links in Spam Email**

Even if the links reads "click to unsubscribe," if that link appears within a spam message, chances are your click to unsubscribe is used solely for the purpose of informing the spammer that your email address is valid, and you may end up on even more spam lists. Delete the emails from your inbox without reading them and move on from there.

Studies indicate that the valid responses from spam is about 1 percent. Clicking any link to get more information or to make a purchase from a spam email is only encouragement for spammers to continue these practices.

Rather than using the links within the spam email, try and find the Web site or service through a search engine or other means. Another alternative would be to find the same or similar service or product from a competitor who is not engaging in spam practices and spend your money there.

**4. Use a Good Email Filter**

The best proactive step you can take to limit spam mail in your in box is to use a good email filter. There are many types of filters available today that will block, or filter email based on its content, header or even language. Most email programs will allow you to define your own criteria for blocking in addition to these filters. There is also a permission-based filter that means you can specify specific email addresses that can send you email. Filters that work at the gateway are extra beneficial in that they can also stop incoming worms and virus email attachments.

**5. Remember the Virus Scanner**

The golden rule for any spam is to never open or accept files from people you do not know. Spam is rife with worms, Trojans, and viruses that can be attached as what seems to be legitimate files in email messages. While the above best practices can help with lowering the number of spam emails you receive, only a real-time virus scanner can help with removing the risks to your system security.

**BEST PRACTICES TO COMBAT PHISHING EMAILS**

**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](https://www.knowbe4.com/?hsLang=en&__hstc=59035826.3fb8202f78a2b930d53fd76aa19e9c34.1548320773345.1548320773345.1548320773345.1&__hssc=59035826.1.1548320773348&__hsfp=2762362733) 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 but if 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,