How to Spot a Fake Website and Not Get Phished

If there’s one thing that cybercriminals excel at, it’s instilling a false sense of trust by taking advantage of our familiarity with current events and playing off mental triggers, such as our feelings of sympathy. We call this “social engineering,” and it’s a key trait in one of the most popular online scams: phishing emails that link to fake websites.

What is Phishing?
Phishing is a form of Internet fraud where a scammer, pretending to be a legitimate person or organization, sends you an email that tries to trick you into revealing personal or financial information, such as credit card numbers, social security numbers, and passwords. Phishing is one of the most common scams on the web and cybercriminals are constantly modifying their attacks to include details that will make the recipient believe the scam is real.

In a phishing attempt, a cybercriminal may send you a message purportedly from your bank, asking you to confirm your account information by clicking on a link. Once you click on the link, it launches a Trojan (a malicious program that appears to be benign) that installs a keystroke logger on your machine. This keystroke logger then captures everything you type, including passwords.

The link may also take you to a fake bank website that asks you to enter your personal information. To the untrained eye, the fake site looks identical to the bank’s real homepage because the scammer has copied files from the real site. However, when you attempt to log in to your account, the site asks for information that the real site never would. It may ask not only for your name and address, but also your account number, password, the last eight digits of your debit card number, and your ATM PIN.

Another common phishing trick that hackers use is erecting fake sites at commonly misspelled addresses in the hope of catching unsuspecting web surfers. Mistyping a webpage address can lead you to these fake sites, an occurrence that’s not uncommon for people who regularly surf the Internet. Creating fake sites is called typosquatting, and like most cyber tricks it’s designed to get your information and your money.

Recognizing Phishing and Fake Websites
The good news is that you can avoid scams by looking for telltale signs that indicate when a site is fake or an email is phishy. The next time you are not completely confident that you are on a legitimate website or that an email you received is valid, check for these signs:

1) **Uses an incorrect URL**—If you are used to going to your bank via a regular address and the address of the site you land at is not the same name, you can be confident that you are not at the real site. Always double check to make sure that the site address is accurate.

   You can also hover your mouse pointer over a link in the email to verify that the link is directed to the same site that the email came from.

2) **Asks for banking information**—A real bank would never ask for your bank account information or your debit card and PIN numbers via email. Be wary of any email or site that asks for sensitive information (such as your social security number) that is beyond your standard login.

3) **Uses a public Internet account**—Before you click on any link sent to you by email, take a look at the sender's email address. If the email is from a public account, but claims to be from your bank or other business, do not trust the email. Moreover, do not trust any email or website that asks you to "confirm" sensitive account information, because this is surely a scam.

   You should also make sure that any email claiming to be from your bank includes your given name in the message, such as "Dear William Smith," instead of "Dear Valued Customer." Real banks address messages to you by name as a way of confirming your relationship.

4) **Includes misspelled words**—If a bank asks you to log in to your "acccount," this is pretty good clue that you've stumbled upon a phishing email or fake website. Real companies have staff checking the accuracy of emails and website, and a mistake like this would be caught before it was sent or published. If you see a misspelling or a misuse of the company name, look for other mistakes and clues to confirm your suspicions—and don't enter any of your personal information on the site.

5) **Is not a secure site**—Legitimate e-commerce sites use encryption, or scrambling, to help insure that your payment information remains safe. You can see if a site uses encryption by looking for a lock symbol in the browser window. Clicking on the lock symbol allows you to verify that a security certificate was issued to that site, a sign that it's a legitimate, trusted website. You should also check that the address starts with "https://" rather than just "http://". Do not enter payment information on any site that isn't secure.

6) **Displays low resolution images—**Scammers usually erect fake sites quickly, and this shows in the quality of the sites. If the logo or text appears in poor resolution, this is an important clue that the site could be phony.

Protecting Yourself
While these tips will go a long way in helping you identify phishing and fake sites, keep in mind that the scammers are always looking for ways to up their game and make their scams more convincing. It helps to be aware of the mental shortcuts you use and to really take the time to ask yourself if the site seems legitimate. Here are some ways in which you can avoid being caught in a cybercriminal's net:

1) **Educate yourself**—Read up on the latest scams so you know what to lookout for. And be familiar with what a phish looks like so you can recognize common tricks when you see them.

2) **Use commonsense**—Read your emails carefully, checking to make sure you know the sender, and be suspicious of any email that asks for your personal or financial information. Also be very cautious when downloading any attachments or files from an email, unless you know and trust the sender.

3) **Practice smart surfing**—When on the web, make sure that the website you're visiting is secure before you enter any information. If you have any doubts, enter a fake password, since phony sites will accept false information. To better protect yourself, you may also want to use a search engine to help you navigate since they can catch misspellings and prevent you from landing on fake websites. Also, use a search tool such as McAfee® SiteAdvisor®, which indicates in your search results whether sites are safe or not.

4) **Use technology to protect you**—Comprehensive security software with anti-phishing technologies, like McAfee SecurityCenter, available pre-loaded on Dell™ PCs, can help protect you. Just make sure that your software is up to date with the latest security protections by enabling automatic updates or clicking the “update” button on your security software control panel.

5) **Be vigilant all the time**—You also want to take precautions when you’re offline, such as monitoring your bank and credit card statements for any suspicious charges or transfers. And consider changing your passwords regularly. Make sure you create strong passwords that use a combination of letters, numbers, and special characters, and that don’t use nicknames, birthdays, or other information that other people may know.

6) **Report anything you think is suspicious**—If you do come across what looks to be a phishing attempt, help yourself and others by reporting it. You can forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov or report phishing scams to the Anti-Phishing Working Group at reportphishing@antiphishing.org.

Although phishing is prevalent, awareness and the right precautions will go a long way in keeping you safe.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com