**Ways to Defend Against Phishing**

1. **Keep your operating system patched to avoid known software vulnerabilities from being exploited.** Install patches from software manufacturers as soon as they are distributed, since hackers can quickly assemble malware using pre-made components to exploit the vulnerability before the majority of people download the fix. A fully patched computer behind a firewall is the best defense against Trojan and spyware installation.
2. **Download the latest version of your browser to ensure that it is also fully updated and utilizes the latest technologies.** Internet Explorer 7 and other browsers include an anti-phishing toolbar to add another layer of protection.
3. **Check the domain name of the site as an indicator of whether the site is legitimate**. The origin of an email, the location of a page, and the use of SSL encryption can all be spoofed. Browser lock icons can also be spoofed. You should ensure SSL is being used (look for “https:” in the URL). Because of hacker tricks, though, you can’t rely on these checks as an absolute indicator that the communication or site is safe.
4. **Never click on links in an unsolicited email, and ignore call-to-action emails such as “Your account will be terminated.”** Call the company on the phone instead, using a phone number that you verify outside of the email.
5. **Be very careful when downloading any software from the web.** Spyware can piggyback onto legitimate software, or the software may contain key loggers or screen scrapers that steal your information. You should completely avoid free screen savers and other freebies. Also be wary of opening an email attachment—a video, graphic, or PDF—even from someone you know. Virus-scanning software protects you by determining if viruses are hiding inside before you open the attachment.
6. **Use software that automatically checks to see whether a URL is safe before you are taken to the site**. Check out **McAfee SiteAdvisor** - a free online safety tool that provides ratings on over 95% of all web sites on the Internet. You can also check the validity of individual web addresses (URLs) with a WHOIS search such as ***www.DNSstuff.com***, which has a search tool that displays the contact information for a domain/IP based in almost any country.
7. **Use an Internet service provider (ISP) that implements strong anti-spam and anti-phishing technologies and policies.** For example, AOL blocks known phishing sites so that customers can’t reach them. The SpamHaus organization (***www.spamhaus.org***) lists the current top-10 worst ISPs in this category—consider this when making your choice.
8. **Review credit card and bank account statements as soon as you receive them** **to check for unauthorized charges.** If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
9. **Be an early adopter of new technologies.** New validation techniques are being used by banks and credit card companies to make online transactions more secure, so make sure to take advantage of them. The computer industry is also working on authentication technologies such as Sender ID, Domain Name, and S/MIME, which will greatly reduce the effectiveness of phishing attacks.
10. **Protect your computer with strong security software and make sure to keep it up to date.** Hackers have databases containing millions of email addresses. They target vulnerabilities in email applications and web browsers, and abuse design vulnerabilities in targeted web site programs. You can defend against phishing, though, because it blends existing techniques of spam and software exploitation.   
    McAfee® Internet Security Suite guarantees trusted PC protection from viruses, hackers, and spyware. Its cutting-edge features include X-Ray for Windows®, which detects and kills rootkits and other malicious applications that hide from Windows and other anti-virus programs. Its integrated anti-virus, anti-spyware, firewall, anti-spam, anti-phishing, and backup technologies work together to combat today’s sophisticated, blended attacks.