Consumer Reports WebWatch
Cybercrime Prevention Project
Fact Sheet #2: Don't Get Phished

This is the second consumer fact sheet in the Consumer Reports WebWatch "Look Before You Click" campaign, supported by a grant from the New York State Attorney General's office, to help educate New York consumers about Internet fraud.

Has this ever happened to you? You get an e-mail that looks like it's from eBay, PayPal or Citibank, asking you to update your account. But don't click on that link! You may wind up on a Web site built by scam artists that downloads a keystroke logger to your home computer that records all your passwords and sends the information to a stranger overseas.

Millions of people have fallen for scams like this – even if they don't do business with the company sending the e-mail. Phishing e-mails usually pretend to originate from financial services companies, Internet service providers or retailers, though some entrepreneurial phishing scammers once even hijacked the name of the U.S. Federal Trade Commission, responsible for prosecuting e-mail fraud.

Depending whom you talk to, the boom in phishing scams has stabilized a bit, but scammers' phishing techniques are improving. Popular social-engineering techniques that entrap consumers include: Associating the mail with a holiday or event, such as the World Cup; spear-phishing, when the sender appears to be someone inside the company you work for; or an e-mail telling you your bank account has been compromised, urging you to enter personal information into a fake site that looks like the bank's.

Here are six tips to help you avoid being phished:

1. Be skeptical of any e-mail, and avoid using hyperlinks in e-mail. They may show one address, but take you to another. Delete any e-mails that seek to send you to a Web page via a link in the e-mail's text. Legitimate e-mails will ask you to go to a specific Web site. Type the address into your browser and make sure what you are typing is the correct address. For instance, Citibank's main site is citi.com, so if an e-mail asks you to type, say, citi.bankloans.com, be skeptical. Make sure your typing is accurate, since cybersquatters buy misspelled domains -- for example, "cittibank.com." Financial institutions are beefing up security against phishing techniques. Bank of America and Vanguard now ask customers to select a personalized image or phrase to appear whenever they access the site to let them know it's the real thing.

2. Make a point to bookmark the pages of the sites you do business with. Use those bookmarks for transactions.

3. On Web pages, mouse over the URL and see whether the address that appears at the bottom of your browser looks related to a page or site you expect to visit. When you arrive at the site, verify that the URL shown in your browser's address bar is the correct one. Pay attention to the part of the URL between "http:// " (or https://) and the next slash. Look for tricks such as the use of a zero where the letter O should be. Verify the address, then type it into your browser. Or use a favorite or bookmark.

4. Watch carefully for misspellings and poor grammar, one of the surest signs of a phishing scam.

5. Use a Web browser with site verification tools, such as Firefox, or software such as McAfee's Site Advisor, which tests sites and tells users the results via a free download.

6. Report phishing. If you receive a phishing e-mail, forward it to the Federal Trade Commission, the Anti-Phishing Working Group, and the company or organization being impersonated. You also can file a complaint with the Internet Crime Complaint Center.

For more information, and to keep up to date on the latest phishing scams and resources for consumers, bookmark Consumer Reports WebWatch.