

What is Phishing?

“Phishing” takes its name from “Password Harvesting Fishing” because it works the same way. The predator sets a lure, hoping that some of the prey will bite the bait and allow themselves to be reeled in. In the case of Phishing, you are the prey and the object of the Phishing expedition is to fool you with a cleverly designed lure, get you to bite, and provide the Phishers with the information they request.

This is Phishing:

Phishing is the use of fraudulent e-mail and Web sites to lure users into revealing personal information, such as passwords, Social Security numbers, account numbers, credit card numbers, and other identifiers.

This is how Phishing works:

Phishing e-mails or Web sites appear to come from trusted sources such as banks, credit unions, retailers or other reputable companies. They usually use official-sounding language and real company logos to make them seem authentic. Typically, they open to a form prompting the recipient to “update” information, and then click a command button to “validate” or “confirm” that the information provided is accurate. The information is then transferred to the creator of the Phishing site and can be used to steal your identity.

This is what Phishing does:

Given the volume of e-mail that can be sent by bulk mailers, a phishing attack can hit millions of people within a few hours. The success rate for phishers is staggering. To make matters worse, while your identity is being stolen, your computer is often being set up for future malicious activities. This is known as Pharming, a technical subterfuge scheme that installs Spyware on PCs to steal data directly, often using keyloggers.

This is how you get Phished:

Phishers can replicate Web sites and other branding of credit unions, banks, merchants and credit card companies so well that an estimated 3%-5% of recipients unknowingly furnish phishers with data. A new, even more devious technique is known as “spear Phishing,” targeted phishing attacks against known members or customers of a particular enterprise. Typically, small to mid-sized institutions are spear-phished, such as regional banks and small credit unions. Spear-phishing yields far higher returns than phishing, typically around 19%, and relies on the customer database being compromised.

To add insult to injury, many Phishing sites host Spyware. Phishing sites often download Spyware onto unsuspecting users, who believe they are replying to requests for information by their banks, credit unions or merchants with whom they do business.

This is how to block Phishing attacks:

- **Be suspicious of e-mails whose subject is “Urgent”, “Urgent Request” or some other eye-catching phrase designed to get you to open it.**
- **Avoid filling out forms that request sensitive data such as passwords, Social Security number, account numbers, or other identifiers that are not public knowledge.**
- **Be suspicious of e-mails claiming to be from financial institutions and other enterprises that are not addressed to you personally. Typically, valid e-mail messages from commercial enterprises are personalized.**
- **Make sure that you are on a secure server if you do submit personal data, such as shopping or banking. In the address bar, look to see that the Web address of the sender begins with <https://>, not <http://>**
- **Validate the address of the sender. In sophisticated Phishing attacks, Phishers implement a floating window over the address bar to hide a fraudulent address. This window is a static image of the company’s legitimate address. Double-click on the address. If it does not “light up”, it is a fraud. Or, try to change a letter in the address. If you cannot do so, it is a fraud.**
- **Ensure that you are running the latest version of your browser, including any security updates.**
- **Install STOPzilla. STOPzilla features advanced Phishing protection. When you navigate to a known or suspected Phishing site, STOPzilla displays a Phishing Alert. You may still go to the site, but it is recommended that you do not do so. To download a free trial version of STOPzilla, go to <http://www.stopzilla.com>.**