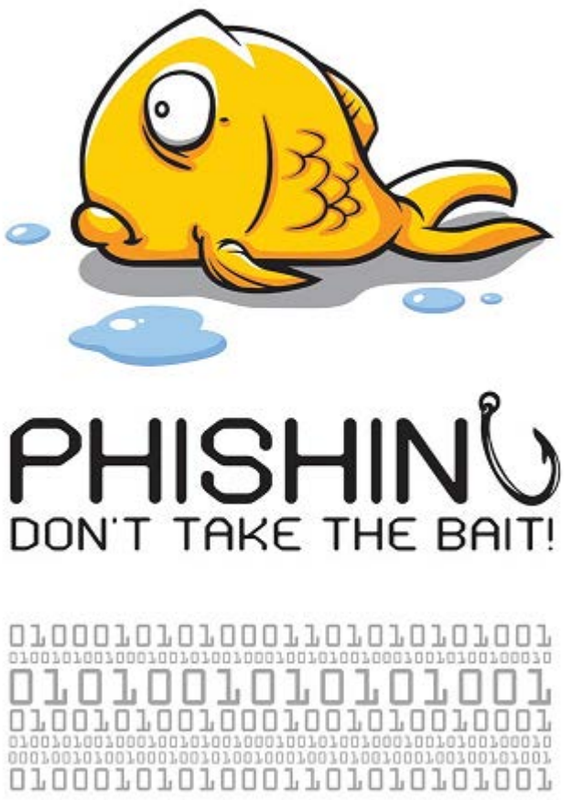
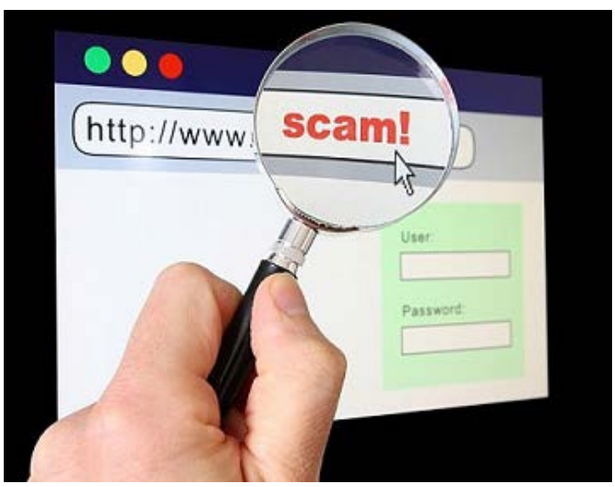
Identity Theft and Fraud Technology Definitions

Keeping up with all the new terms being used to describe the different types of identity theft, fraud, and security breaches can be confusing! This definitions list is a quick reference to that terminology.



Phishing is the attempt to acquire information such as usernames, passwords, or other sensitive information from someone by pretending to be a trustworthy entity. Phishing is usually carried out via email, instant messaging, or other electronic communication. Some phishing emails direct the recipients to websites that look like legitimate websites, in an attempt to lure them into entering their usernames, passwords, etc., into a login page. Credentials entered by the victim are then captured and used to access the victim's accounts, or used for identity theft, etc. It is also common for phishing emails to try to entice the recipient to click on links that are designed to cause malware to be downloaded unto the victim's computer. In a workplace environment, phishing can enable an attacker to install malware on a recipient's computer, and the attacker can then use the malware to ultimately gain privileged access to the organization's network resources. *(By the way, you should not even click on a link that purports to be an "unsubscribe" link in an email message. Instead simply delete the email message itself)*.

Spear phishing is a more specifically targeted form of phishing in which the email or communication contains information that could lead the victim to believe that the communication is from someone he or she knows, and therefore, can trust. A spear phishing email, rather than addressing the recipient generically, could appear to come from the recipient's bank or financial institution, a friend of the recipient, a legitimate company, government agency, an educational institution, etc. It typically addresses the recipient by his or her actual name, and might contain additional personal information to lead the recipient to believe that the sender is an entity or someone they have an established business or personal relationship with. For this reason, more recipients fall victim to spear phishing. It is therefore considered more effective, and therefore, more dangerous than regular phishing. Some attackers first carry out phishing attacks in order to obtain more specific information to use in spear phishing attacks.

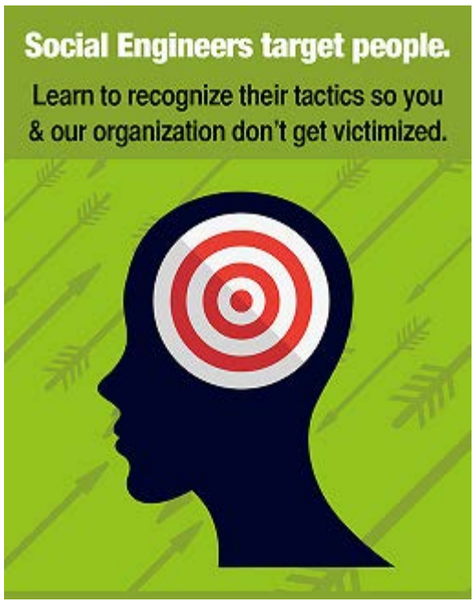


Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

Always ensure that, once the page has loaded, that the URL is spelt correctly and hasn't redirected to a slightly different spelling, perhaps with additional letters or with the letters swapped around.

Antivirus software can also help to protect against pharming instances, especially when you enter an unsecured site without realizing. Keeping this up-to-date will help to fight against pharming.

Never provide your personal, credit card or account details online unless you have verified the website is authentic.



Instead of attacking a computer, **Social Engineering** is the act of interacting and manipulating people to obtain important/sensitive information or perform an act that is latently harmful. To be blunt, it is hacking a person instead of a computer. Social engineers can the use the phone, the internet, or even show up in person to perform the malicious act. They can be after data such as ID number, username, password, server names, machine names, remote connection settings, schedules, credit card numbers, etc. They may also try to get someone to install some malicious software, visit an unscrupulous website, or even access unauthorized locations.

Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a Caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious by the speaker or writer.