Types of Fraud

Phishing

A form of identity theft in which a scammer uses an authentic-looking e-mail to trick recipients into giving out sensitive personal information, such as a credit card numbers, bank account numbers, Social Security numbers or other sensitive personal information.

Vishing

Voice phishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Voice phishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP makes formerly difficult-to-abuse tools/features of caller ID spoofing, complex automated systems (IVR), low cost, and anonymity for the bill-payer widely available. Voice phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

SMiShing

In computing, SMS phishing or smishing is a form of criminal activity using social engineering techniques. Phishing is the act of attempting to acquire personal information such as passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. SMS (Short Message Service) is the technology used for text messages on cell phones.

SMS phishing uses cell phone text messages to deliver the bait to induce people to divulge their personal information. The hook (the method used to actually capture people's information) in the text message may be a website URL, but it has become more common to see a telephone number that connects to an automated voice response system.

Identity theft

Even if hackers don't steal from your account, it can be compromised by identity theft. ID thieves can capture your personal information, such as your Social Security number, and other identifying data. That data could be used to create new accounts in your name or hack into your other accounts.

Keylogging

If you access your online banking site on public networks, such as Internet cafes or public Wi-Fi, there is a chance that you could fall prey to keylogging. Keylogging uses software that records your keystrokes to get your account details.

Pharming

This might be a little more difficult for hackers to carry out, but it does happen. Pharming occurs when hackers are able to hijack a bank's URL so that when you try to access your bank's website, you get redirected to a bogus site that looks like the real thing.

Trojans

Programs that perform malicious actions but have no replication abilities. Like the original Trojan horse, these programs may arrive as seemingly harmless files or applications, but actually have malicious intent within their code. Banking Trojans are specifically designed to gain control and compromise online accounts.

Site spoofing

Websites that appear professionally designed and legitimate with the purpose of collecting sensitive information from unsuspecting visitors.

Social engineering

In the context of information security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or gaining computer system access. It differs from traditional cons in that often the attack is a mere step in a more complex fraud scheme.

Caller ID spoofing

Is the practice of causing the telephone network to display a number on the recipient's Caller ID display that is not that of the actual originating station. The term is commonly used to describe situations in which the motivation is considered malicious by the speaker or writer. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, Caller ID spoofing can make a call appear to have come from any phone number the caller wishes. Because of the high trust people tend to have in the Caller ID system, spoofing can call the system's value into question.

Email spoofing

Is email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and forge emails.

Although there may be legitimate reasons to spoof an address, these techniques are commonly used in spam and phishing emails to hide the origin of the email message.

Man-in-the-browser (MITB, MitB, MIB, MiB)

A form of Internet threat related to man-in-the-middle (MITM), is a proxy Trojan horse that infects a web browser by taking advantage of vulnerabilities in browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host web application. A MitB attack will be successful irrespective of whether security mechanisms such as SSL/PKI and/or two or three-factor Authentication solutions are in place. A MitB attack may be countered by utilising out-of-band transaction verification, although SMS verification can be defeated by man-in-the-mobile (MitMo) malware infection on the mobile phone. Trojans may be detected and removed by antivirus software with a 23% success rate against Zeus in 2009, and still low rates in 2011. The 2011 report concluded that additional measures on top of antivirus were needed. A related, more simple attack is the boy-in-the-browser (BitB, BITB). The majority of financial service professionals in a survey considered MitB to be the greatest threat to online banking. For online banking, using portable applications or using alternatives to Microsoft Windows and Mac OS X like Linux, Chrome OS or mobile OSes may be the safest, especially when run from non-installed media.

Skimming

Card skimming is when someone illegally copies your debit card data from the magnetic strip. There are many ways a person can do this and being aware of the machines you are using can help prevent becoming a victim. If you inadvertently use a compromised machine, what may seem like a harmless ATM withdrawal or debit transaction can turn into your entire bank account being drained of your hard earned money. How? Scammers put small, inconspicuous contraptions that many of us would over look over keypads and swipers, resulting in your information being stolen within seconds.