POPULAR BANK

Information Security Guide
Security Slopes

TYPES OF FRAUD

DELIVERY OF INFORMATION TO THIRD PARTIES

Pharming - Webpage Redirection

It is a practice consisting of redirecting you from a page on the Internet, by manipulating your email address to another false page, created with the aim of defrauding you, collecting your confidential data. Pharming is especially dangerous since the user is not aware that is being redirected to a fake page.

Phishing - Electronic Fishing

It is the sending of emails to supplant the identity of a bank or virtual commerce entity, and thus obtain their confidential data under the allegation that:

- Require quick confirmation of your personal and confidential data.
- They insist on updating their personal and confidential data.
- Warn that your financial product(s) will be cancelled if you do not submit the information requested.
- Irresistible offers for an exaggeratedly limited time, creating the illusion of opportunity.
- They inform you that new payees have been added to your accounts.

Because the email message is mass-sent to the fraudsters' pool of email addresses, many recipients aren't even customers of the spoofed entity.

Smishing - Cell Fishing

It derives from combining SMS and phishing and is just another form of deception through SMS messages to the mobile phone. A criminal sends you a text message to induce you to provide your financial information; it can also ask you to click on a link to, in the end, steal the data that you have naively provided and carry out the fraud.

Vishing – Telephone Fishing

Vishing is a fraudulent criminal practice where the Voice over IP Protocol (VoIP) and social engineering are used to deceive people and obtain sensitive information such as financial information or information useful for identity theft.

ATTACK VIA PROGRAMS OR EQUIPMENT

Keylogging - Capture keys

It derives from the English key and logger. They are malicious software designed to record keystrokes, store them in files and send them to their creators.
These programs can be distributed through a Trojan or as part of a computer virus or worm.

Malware - Malicious program

Abbreviation for malicious program, malicious software, by its definition in English. These programs include viruses, spyware, Trojan, worms, keyloggers, etc., which are designed to infiltrate, auto-run, damage a computer's operating system, steal information, etc.

Skimming - Card Capture

It refers to a device that is installed in the slots of the ATM to capture the information of the magnetic stripe on your debit or credit card, as soon as you introduce it. Sometimes it works in conjunction with a hidden camera or a transparent keyboard, which is overlaid on the ATM keyboard, to capture your PIN.

Spyware – Spyware Program

Within the malware category, it is the type of program that is installed on a computer by downloading or installing a program. These programs perform different functions, such as displaying unsolicited advertisements (pop-up), collecting private information, redirecting page requests, etc.

MAN IN THE MIDDLE

Eavesdropping – Secret Listening

Term that refers to someone who secretly listens to what is said in private. In the context of security, it is applied to eavesdropping attacks to obtain information.

Sniffing – Online Capture

Sniff or sip, for its meaning in English.
They are applications designed to capture frames (traffic) in networks and store them for later analysis, without needing to have access to any network system.

There are two kinds: software sniffing and hardware sniffing. The first is a program that captures online information, and the other is a device installed on or near a computer to interfere with its data transmission.

Spoofing - Data Simulator

In terms of network security, it refers to the use of identity theft techniques, generally with malicious or for investigative uses.

Reply attack - Intercepted mailings
It is an attack in which a data packet is intercepted and forwarded to the receiving server. Thus, a hacker intercepts the communication and can obtain the username and password that allows him to enter a system without authorization.

OTHER STRATEGIES

Carding - Card Hunting

It refers to the unauthorized and massive use of debit and credit cards to fraudulently acquire goods and services. The term has recently evolved to include a whole set of activities surrounding the theft and use of card numbers for fraud such as pharming, phishing, scamming, skimming, smsishing, spoofing, etc.

Scamming – Trick

Synonym of scam, fraud.

It works when the user receives an email through which he is promised a job, a large sum of money, expansion of his personal relationships, etc., where he is asked to open a bank account to receive money and transfer it to other accounts, receiving commissions for this task.
The scam has its origin in hoaxes, or email chains, with false and misleading content whose topic used refers to be incurable diseases, chains of solidarity or luck, urban legends, etc.

“Spamming- Unexpected emails

Unexpected emails This is the name given to unsolicited email messages from unknown sender, usually of an advertising nature, which are sent in massive amounts. It affects the recipient when it overwhelms their mailbox and consumes their bandwidth unnecessarily.
Behind the spam there is also false advertising that encourages the customer to buy products that will not be received, spreading phishing or malware.