FRAUD Awareness

PACIFIC CONTINENTAL®
THE RIGHT BANK®

Glossary of Terms

Learn more:

Want to learn more about fraud and how to protect yourself and your business?

Sign up to receive Pacific Continental Bank's quarterly Fraud Awareness *eTips* eNewsletter.

eTips offers helpful and timely information on current fraud trends and what you can do to safeguard against them. Learn more at therightbank.com.

Account Hijacking – A cyber criminal captures a user's login credentials using a keystroke logger or remote access Trojan to gain access to the ACH origination system, and then uses the credentials to make fraudulent payments.

Advanced Persistent Threats (APTs) - Attack that uses multiple phases to break into a network, avoid detection and harvest valuable information over the long term.

Adware – A type of software that often accompanies free downloads; some types display ads on your computer, while others monitor your computer use (including websites visited), and then show targeted ads based on your usage.

Advanced Fee Fraud (AFF) – A common scam in which a fee is demanded from the victim in advance of the victim receiving a lottery winning, a loan, money from a deceased relative, etc.

Anti-Virus Software – Software that protects a computer from viruses that can potentially destroy data, slow the computer's performance, cause a crash or even allow spammers to send emails from an associated account.

Authenticate – Function used to verify the identity of one of the following: a user, user device, other entity or the integrity of data stored, transmitted or to establish the validity of a transmission.

Back Door – Hidden software or hardware mechanism used to circumvent security controls; synonymous with trap door.

Blacklisting – Maintaining a list of undesirable applications and preventing them from running.

Botnet – A network of computers that scammers have infected with hidden software to secretly send spam.

CAN-SPAM Act – Law that prohibits senders of unsolicited commercial email from using false or misleading header information or deceptive subject lines. It requires the sender to identify each email as an advertisement, among other provisions.

Card Skimmer – Illegal electronic device which can capture all of the personal information from a credit card or debit card.

Cashier's Check – A check from a bank's own account; these are easily counterfeited. Always confirm all aspects of the check with the issuing bank and the holder of the account before considering it valid.

Check Kiting – When someone writes a check for an amount that exceeds their account's balance and then deposits a check from another account that also has insufficient funds to "cover" it.

Cookies – Small text file that a website can place on a computer's hard drive to collect information about activities on the site.

Counterfeit – Made in exact imitation of something valuable or important with the intention to deceive or defraud.

Cramming – The illegal placement of unathorized charges on your telephone bill for unrequested services or calls that were not made.

FRAUD Awareness CONTINUED ON NEXT PAGE >

CryptoLocker Virus – A virus that originates from emailing a PDF attachment that, once opened, installs malware on your hard drive and allows hackers access to your computer files. This virus then seizes control of those files and threatens to erase them unless you pay a ransom.

Data-Driven Attack – A form of attack that is encoded in seemingly innocuous data, which is executed by a user or process to implement attack. A data-driven attack is a concern for firewalls since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Denial-of-Service (DoS) Attacks – These attacks overwhelm a website's servers by flooding them with requests which makes the website unreachable or unresponsive.

DNS Spoofing – This attack assumes the domain name system (DNS) of another system by either corrupting the name service cache of a victim's system or by compromising a domain name server for a valid domain.

Drive-By Download – Software that installs on a computer without the user's knowledge when visiting certain websites.

Dual Controls – A security procedure requiring two people (or possibly two processes or devices) to cooperate in gaining authorized access to a system resource (data, files, devices, etc.).

Embezzlement – The act of taking money for one's own use in violation of another's trust.

Encryption – The scrambling of data into a secret code that can be read only by software set to decode the information.

Filter – Software that screens information on the Internet, classifies its content and allows the user to block certain kinds of content.

Firewall – Software or hardware that helps screen out hackers, viruses and worms that try to reach computers over the Internet.

Forgery – The act of making or producing an illegal copy of something so that it looks genuine, usually for financial gain.

Hacker – Someone who uses the Internet to access computers without permission.

Hardcover Insurance Policy – Term made up by scammers to persuade victims to pay additional fees to receive a fake prize or winning.

Identity Theft – The fraudulent use of another person's identifying information, such as name, social security number, bank account or credit card number for the thief's own personal gain.

Internal Controls – Systematic measures, such as reviews, checks and balances, methods and procedures instituted by an organization to help prevent and detect fraud.

Keystroke Logger – Device or program that records each keystroke typed on a particular computer.

Malicious Code – Any code or part of a software system or script that is intended to cause undesirable effects, security breaches or damage to a system.

Malicious Insider – Threat to an organization from a current or former employee, contractor, or other business partner who currently has or previously had authorized access to an organization's network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity or availability of the organization's information or information systems.

Malware – Software designed to cause harm on the computer in which it is installed.

Man-in-the-Middle – This attack intercepts communication between two systems. The attacker splits the original transmission control protocol (TCP) connection into two new connections, one between the client and the attacker, and the other between the attacker and the server. Once intercepted, the attacker can read, insert and modify the data in the intercepted communication.

Money Laundering – The practice of engaging in specific financial transactions in order to conceal the identity, sources and/or destination of money.

Multi-Factor Authentication – An approach to security authentication which requires the user of a system to provide more than one form of verification in order to prove their identity and allow access to the system.

Pharming – An attack in which a user can be fooled into entering sensitive data, such as a password or credit card number, into a malicious website that impersonates a legitimate website.

FRAUD Awareness CONTINUED ON NEXT PAGE >

Phishing – Type of scam with the intent of capturing personal information such as Social Security numbers, online banking user identification numbers, debit and credit card account numbers and passwords.

Ransomware – A malicious computer program that restricts or disables your computer and then demands, typically via a pop-up window, that you pay a fee to fix the problem.

Reverse Phishing – A type of scam where cyber-criminals send emails to businesses with fraudulent banking information, redirecting payments to an account they control.

Scareware – A type of malware that displays on-screen warnings of nonexistent computer infections or generates constant pop-ups intended to trick you into buying useless or potentially dangerous "protection" software.

SEO Poisoning – Strategy in which hackers isolate keywords that generate buzz on Google and other search engines and then create malicious URLs about the topic so that search engines index it alongside other results. These pages then download malware on to the visitor's computer.

Social Engineers – Criminals who take advantage of human behavior to gain access to data or infiltrate businesses.

Spam – An unsolicited, often commercial, message transmitted through the Internet as a mass mailing to a large number of recipients.

SMiShing – A type of scam where a cyber-criminal contacts a victim via text message, directing them to call a toll-free number or visit a website which asks for the victim's personal or financial information.

Spear Phishing – Type of phishing usually directed at a person within a company who is able to initiate business funds transfers or payments. A cyber criminal sends an attachment containing a keystroke logger, which will capture the user's online banking credentials and transmit them back to the criminal.

Spyware – Software that collects information about a person or organization without their knowledge or informed consent and reports such data back to a third party.

Timthumb Attack – Attack in which hackers exploit a security flaw in a popular file used by Wordpress and other website-building platforms to crop and resize images (Timthumb.php) and install malicious code or files into a website server. This allows the hacker to launch spear phishing campaigns and denial-of-service attacks.

Trojans – Programs that, when installed on your computer, enable unauthorized people to access it and potentially send spam from the device.

Vishing – Short for "voice phishing," it's the use of recorded messages to telephones, usually claiming to be from a bank, with the goal of tricking you into revealing personal or account information for identity theft.

Virus – Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Whitelisting – A computer administration practice used to prevent unauthorized programs from running. The whitelist is a list of applications that have been granted permission by the user or administrator. When an application tries to execute, it is automatically checked against the list and, if found, allowed to run.

Worm – Independent program that replicates from machine to machine across network connections, often clogging networks and information systems as it spreads.

FRAUD Awareness

Connect with us.

GREATER EUGENE
541-686-8685

GREATER PORTLAND
503-350-1205
360-695-3204

GREATER SEATTLE
206-676-8880
425-688-3793
253-552-4800

TOLL-FREE
877-231-2265

EMAIL
banking@therightbank.com

WEBSITE
therightbank.com

SOCIAL

#PCBfraudawareness