Trends in Fraud, phishing, social engineering: Risk Mitigation

Author: Brent Meyers

Fraud is explained as wrongful or criminal deception intended to result in financial or personal growth. An individual or thing intended to deceive others by unreasonably claiming or being credited with accomplishments or qualities. Here are the current fraud trends.

1. Malwares
Malicious + Software = Malware. Code or software that is specifically designed to damage, disrupt, steal or inflict some other “bad” or illegitimate action. The majority of malware infections caused by some action from a user like clicking an email attachment or URL, downloading a file from the internet, viruses, worms, Trojans and botnets.

2. Phishing
A fraudulent attempt usually made through email, to filch your personal details. Phishing emails usually emerge from a well-known organization and ask for your personal information. It is possible that these attempts will appear to come from an organization or person that you do business with or know personally. Phishing started out as a way to acquire user ids, password, and other confidential data. These credentials are then used to logon to the online applications (i.e. internet banking) and transfer funds to other “money mule “accounts. The two types of phishing are 1) Spear Phishing-Targeted Phish against a specific organization, 2) Whale Phishing-A spear Phishing attempt that targets the CEO or high level executive of a company.

3. Social engineering
The act of manipulating people into performing actions or divulging sensitive information. Social engineering is typically carried out face-to-face, by phone, or email. Social Engineering used to require more manual tasks to be successful. Evolved from Nigeria Scams to ‘Visa Fraud Department’, hacked Gmail, AOL accounts. Social Networking makes it easy to provide real information about the victim.

4. Steps to Prevent Fraud
The key steps to prevent fraud are: Be proactive, establish hiring procedures, train employees in fraud prevention, conduct regular audits and call in an expert.

5. Best practices
The best practices to prevent fraud are: Dedicating a personal computer for online business transactions and block all email and other web browsing capabilities from the PC. Use dual-control for ACH and wire payments. Dual control approvals should be conducted from separate PCs. Monitor and reconcile accounts daily. Deploy white-listing software and web monitoring and filtering capabilities. Block URL shortening services and access to social networking sites. Implement SPAM filtering on inbound email to block unsolicited email. Disable hyperlinks from incoming email messages so they cannot be selected.

Related Webinars
Accounts Payable Payment (ACH, Check, and Card) Fraud, Risk and Risk Mitigation

Top Articles
Using Excel Spreadsheets in FDA Regulated Environment
How to Identify and Avert Procurement Fraud
10 Steps to Fight Cyber Fraud
Basic Red Flag Audit-Detection Methods and common red flags in procurement frauds
How do Banks comply with NACHA Operating Rules