

First Friday Fraud Facts+

February 3, 2012

The Idaho State Controller's Office distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.



QUESTIONS OR COMMENTS:

Matt McBride, CGFM
Financial Specialist

P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8805

Fax: (208) 334-3415

E-mail: mmcbride@sco.idaho.gov

Inside this issue:

Welcome	1
Social Engineering	1
Best Practices	2
Fraud Case	2
Fiscal Focus	3
Technical Tip	3
Announcements	3

Welcome to First Friday Fraud Facts+ (F⁴⁺ now includes topics in addition to fraud). This edition will cover a scheme used by fraudsters to obtain sensitive information. The scheme is referred to as social engineering.

SOCIAL ENGINEERING

The term "social engineering" refers to schemes employed to acquire sensitive information stored on a computer. The fraudster tricks someone with valid access to a computer system into allowing the social engineer improper and unlawful entry into systems and files.

Social engineering relies on the unjustified trust and helpfulness of those with valid access to information and systems. The fraudster takes advantage of the confusion caused by an ever-changing technological environment or the failure of those with valid access to understand the value of the information and the harm that a social engineer can cause by using illegally acquired information.

A typical social engineering scheme would involve the wrongdoer posing as a member of an organization's IT staff. He or she would, for example, call random numbers at a government entity claiming to be calling back from technical support. Eventually the perpetrator will connect with an employee who happens to have a legitimate problem and who is grateful that someone is calling back to help. The social engineer will "help" solve the problem and in the process have the employee divulge his/her password, disclose confidential information, or type commands that give the criminal access to the system. The social engineer is the con man of the twenty-first century.

Before divulging a password or what might be confidential, sensitive or privileged information an employee should ask:

- Am I following my organizations guidelines for releasing information?
- Should this information be released to the public and, if so, under what circumstances and with what controls?
- Has the person requesting information been properly identified and is that person entitled to receive the information?



- Can the information be inappropriately used to access other records, gain entry to secure systems, or cause harm to the government or citizens?

BEST PRACTICES

Organizations must be vigilant in their efforts to safeguard the considerable amount of sensitive information that is in their possession. Such efforts include:

- Developing protocols for dealing with information requests
- Practicing "Professional Skepticism"
- Identifying and communicating to employees which information is confidential or sensitive
- Training employees to verify the identity of anyone who requests confidential or sensitive information
- Periodically testing all aspects of system security, including the reactions of employees to requests for confidential or sensitive information

SOCIAL ENGINEERING FRAUD CASE

A multi-million dollar, international fraud and money laundering scheme targeted vendors of state governments from West Virginia, Kansas and Ohio, as well as the Commonwealth of Massachusetts, which resulted in the diversion of nearly \$3.4 million in state payments routed to fraudulent bank accounts.

The fraudsters were able to hijack legitimate vendor payments using information acquired through the Internet and other areas to complete direct deposit authorization forms for deposits to fraudulent accounts that appeared to belong to major government vendors. The fraudsters:

- Targeted state vendors that routinely received significant payments
- Created phony entities with names similar to the legitimate vendors
- Produced fraudulent bank accounts in the names of the targeted vendors
- Mailed authorization forms and voided starter checks from fraudulent accounts
- Received payments from unsuspecting states that were sent to fraudulent bank accounts

FISCAL FOCUS—SHARING PASSWORDS

Sharing passwords is never a good idea.

You are sharing your identity when you share your password. A password is like your signature and is the only way a computer has to identify you.

Sharing passwords muddles the audit trail. You should always be able to tell specifically who logged into what and when. If you happen to share your password with someone who embezzles funds, you would be considered a suspect in a crime because your name would be associated with those transactions. Even if you were able to clear your name, you would know that you created the opportunity for another person to commit a crime.

The likelihood of errors and omissions also increases when you share your password with untrained personnel. No one needs to know your password, including your assistants, supervisor, or technical support personnel. They have the access they need to perform their duties.

When access is needed, specific usernames and passwords should be required for each employee. Permission to use resources can be granted, modified, or revoked depending on the particular access an employee needs to perform their job.

TECHNICAL TIP

Just as criminals adapt to the evolving technical landscape we must also adapt. This doesn't necessarily mean you need to be a firewall guru or be well versed in the art of security kung-fu. What it does mean is you need to spend a little time and apply some common sense to every day types of events just as you would lock your car doors when you park your car on a busy city street.

The link provided below gives some helpful tips on securing your home wireless network, written in an easy to read format without all the technical jargon. These steps can go a long way to help protect you from becoming a fraud victim by securing your home network.

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201201_en.pdf

ANNOUNCEMENTS

Mark your calendars to attend one of the following Idaho SCO's Annual Internal Control Training sessions:

a) Tuesday, April 3, 2012, from 8:15 a.m. — 10:15 a.m.

OR

b) Thursday, April 5, 2012, from 8:15 a.m. — 10:15 a.m.

