

First Friday Fraud Facts+

January 1, 2016



QUESTIONS OR COMMENTS:

Chris Floyd, CPA
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8814
Fax: (208) 334-3415
E-mail: cfloyd@sco.idaho.gov

Inside this issue:

| | |
|--|---|
| Welcome | 1 |
| The Original Trojan Horse | 1 |
| Modern Day Fraudsters | 2 |
| What a Social Engineer Might Say or Do | 2 |
| What Can I Do? | 3 |

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.

Welcome to First Friday Fraud Facts+ (F4+). This edition will discuss social engineering.

The term "social engineering" is defined both traditionally and in relationship to technology:

- Traditional: "the manipulation of the social position and function of individuals in order to manage change in a society"
- Technology: "...cracking techniques that...aim to trick people into revealing passwords or other information that compromises a target system's security"¹

Perhaps a more encompassing definition could be, "the art and science of getting people to comply to your wishes through the use of psychological tricks."² While not perfect, our defensive measures in life are quite robust and continually evolving. Fraudsters have had to adjust their tactics from *forcing* their way into our safe havens to tricking us in to opening the door for them by exploiting our human tendency to trust.

The Original Trojan Horse

Although presumed more fictional than fact, perhaps the most famous account of social engineering is the account of the Trojan Horse. The Greeks had laid siege, but could never gain access, to the city of Troy for 10 years. Seemingly weary of the siege, the Greeks built an offering of goodwill for the goddess Athena and appeared to sail away toward their homeland.

The Trojans, thinking they had finally driven off the Greeks, accepted the "gift" and brought it within the walls of what had, up to that point, provided an impenetrable safe haven. In the dark of night, the elite force hidden within the belly of the horse exited, signaled the waiting Greek force that had returned under cover of darkness, and then opened the doors of the city. This seemingly innocuous act of accepting a gift led to the





Courtesy of sans.org

decisive end of the war.

The success of the Greeks' plan centered on the Trojans accepting an offering of goodwill. The Trojans, perhaps dulled from years of battle, willingly accepted the gift as a spoil of war.

Modern Day Fraudsters

Fraudsters have evolved over the years to more advanced, more complex methods of gaining unauthorized access to a person's or an organization's resources. As illustrated in the story of the Trojan Horse, modern fraudsters are creative, patient, and great actors, and focus their attacks at the physical and psychological levels.²

Most scams follow a four-stage method:

1. Information gathering (creative)
2. Relationship development (patient)
3. Exploitation
4. Execution (actors)³

Social engineers can attack through malicious phone calls, dumpster diving, or online harvesting of information. They will spend days or weeks getting to know their targets by looking for information anywhere they can. Much of the information they glean appears to be harmless and useless. Individually, a phone number or an address may not provide much information that could lead to identity or information theft. However, what kind of information does a credit company request when a person calls to reset a personal identification number in order to validate the operator is speaking to the account holder? "What is your account number? What are the last four digits of your home phone number? What is your zip code?"

What a Social Engineer Might Say or Do

- On the phone, a social engineer might call and pretend to be a fellow employee or a trusted outside authority such as a law enforcement officer or an auditor. We tend to trust authority figures, particularly when they sound or look legitimate.
- Someone behind you walks in after you open the door using your security badge or asks you to hold the door because they "forgot" their access card or their arms are full. The person holding the door is simply trusting in their desire to be a good neighbor.
- Hackers have begun sending emails that appear to originate from known friends or colleagues. The name associated with the email address is familiar; however, the email address itself belongs to the hacker. We trust that when a familiar name shows up in our email box that the message is legit.
- Hackers hold a computer ransom by using encryption software (ransomware) that infected the system when the user clicked on a link embedded in a phishing email or as they "drove by" an infected website.

Once encrypted and inaccessible, a message appears instructing the user to pay a ransom fee to release the files. We tend to trust that the physical and electronic countermeasures put in place are enough to fend off illicit hackers.

What Can I do?

Here are a few suggestions on how to combat social engineering⁴:

- Do not use email out of office replies, auto-responders, or vacation settings tools. If you do, keep the information you provide as vague as possible.
- The age-old never click on an email link from someone you do not know.
- Do not assume the unfamiliar person on the other end of the phone is who they purport to be. Remember the Australian radio host who obtained personal medical information about the Duchess of Cambridge by pretending to be the Queen of England over the phone?
- If your workplace uses security badges, do not let anyone through the door without one. Being a good neighbor also entails keeping your workplace safe.
- Lock your computer before walking away from your workstation.
- Protect your personal information - all of it. Shred it. Delete it. Do not give it away.



Courtesy of thehackernews.com

¹ Social engineering as defined at dictionary.com.

<http://dictionary.reference.com/browse/social%20engineering?s=t>. Accessed 13 May 2015.

² *Social Engineering Fundamentals, Part I: Hacker Tactics*. Sara Granger. 3 Nov 2010.

<http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Updated 3 Nov 2010. Accessed 24 Apr 2015.

³ *Guide to Preventing Social Engineering Fraud*.

<http://www.chubb.com/businesses/csi/chubb19441.pdf>. Accessed 18 May 2015.

⁴ *Social Engineering - Five Best Practices for Defending Yourself*. Joshua Wilson. 10 Jan 2013.

<https://www.neustar.biz/blog/social-engineering-5-tips-best-practices>. Accessed 18 May 2015.