

## **IMPORTANT SECURITY NOTICE**

October 11, 2011

**Don't Become The Victim Of a Social Engineering Attack.** Social engineering is the art of manipulating people into performing actions or divulging confidential information. There are many types and variations of social engineering attacks. Most of these are conducted remotely, either by telephone or the internet. However some social engineering attacks are conducted in-person. In this document, we will provide some recommendations to mitigate these types of attacks.

### **Recommendations To Protect The Company & Yourself From Social Engineering Attacks:**

1. Carefully inspect all emails before opening. Suspicious looking emails from anonymous sources or domains such as gmail or yahoo, etc. should be deleted and not opened.
2. Emails from people you know...but that otherwise look suspicious should not be opened or acted upon. For example, you receive an email from a friend that simply contains a web link or file and no message. Or a message that is unlike a typical message from your friend. Assume that your friend's email account has been compromised and that you will receive a virus or other malware if you click on the link or open the attachment. Do not open unless you have verified with your friend or co-worker that they did in fact send you this message.
3. Often these social engineering attacks originate from third-world foreign countries. Emails that contain mis-spellings, mis-nomers, odd questions or statements, etc. should not be responded to and should be deleted. Example: "I am liking your POS systemEs and would like to buy qty 14 of these with my Visa card and I will come and pick them up."
4. Unsolicited emails that sound too good to be true usually are. Example: Do not respond to an email advising you that a person you do not know has just passed away and left you \$20m...and all you have to do is give us your bank account information...etc.
5. A favored social engineering attack is to send an official-looking email stating that there is something wrong with your account and advising you that your service may be interrupted if you don't quickly provide certain information. Legitimate companies are not going to arbitrarily send you an email asking you to enter private information such as your birth date, social security number, credit card number, bank account number PIN, password, etc. Even if the email or web link appears to be legitimate, do not provide private information as a result of an unsolicited request via email.

*Page 1 of 3*



6. Do not provide any personal information or confidential company information to anyone on the telephone. No legitimate company representatives should be contacting you by telephone to obtain any personal or company information. No one from IT or tech support should ever call you and ask you for your network user name or password, IP or Mac address, birth date, social security number, drivers license number, address, etc. Do not provide any confidential information to anyone on the phone unless you can verify the legitimacy of the caller. For example, if someone calls you claiming to be from the HR department and asks you for personal information, get their name and phone number. Contact the HR department and verify this is a legitimate employee and the request is legitimate. If you cannot confirm the legitimacy of the caller, do not provide any information.
7. Do not answer any questions from unsolicited callers or emails about the company systems or infrastructure. Examples: If a caller or email sender represents themselves as a salesperson and asks you what kind of phone system, or CRM, firewall, anti-virus, anti-malware, intrusion detection, file integrity management, etc. system we use...**do not** provide this information. You may be helping an attacker gain important information about the company's IT infrastructure.
8. In some cases, an attacker may call and inform you that they have the wrong extension and ask to be transferred to someone else. Do not transfer these callers. Instead, instruct them to hang up and call the switchboard.
9. In some cases a caller may ask you to give them an outside line. Do not do this. Advise the caller to hang up and call the switchboard.
10. If an unsolicited caller identifies themselves as a repair vendor and asks you to do something, politely refuse. Example: I am the AT&T rep and I need you to punch a few buttons for me.
11. Do not answer unsolicited emails from people representing themselves as vendors asking you to point them in the right direction. Examples: I am looking for the name and contact information for the person in charge of IT...or HR...or Security...etc. Do not provide this information, as you could be assisting a social engineering attacker.
12. Look for tell-tale signs of social engineering...such as urgency, (you have to act now!!), name-dropping, intimidation, refusal to give you their contact information, requests for forbidden information or things that just don't make sense or sound right. Do not respond with the requested information. Consult your manager if you question anything.
13. Avoid social networking sites if possible, as these are favored places for social engineering attackers. If you use social networking sites, refrain from listing private information that an attacker could use against you. Don't log your birthday on Facebook, for example.
14. No company business should be conducted on any social networking sites.

15. Anyone entering a company facility should display an identification badge. A favorite method for social engineering attackers to gain entrance to your place of work is by “Tailgating”, or entering a building behind a legitimate employee. Make it a point to check people coming in the door for their badge. If you don’t see one and don’t recognize the person...., challenge them. Ask to see their badge. If they can’t produce a badge, escort them to the guard desk.
16. Do not allow other people to look over your shoulder while you are entering your user name/password.
17. Do not allow other people to use your computer.
18. Do not connect a removable media device, such as a thumb drive, portable hard drive, disk, etc, that you found lying around to any company computers.
19. Do not connect any removable media you receive unsolicited through the mail or a parcel service to any company computers.
20. Do not discard any paper or electronic media that contains any sensitive information in the trash. The company provides receptacles for these...please use them.
21. Promptly report any suspicious persons or activity to the guard at the security desk.