MD INFRAGARD
INSIDER THREAT SPECIAL INTEREST GROUP

Tips For Employees And Employers
How To Handle Social Engineering Attacks

May 19, 2013

Tips For Employees And Employers On How To Handle Social Engineering Attacks

The common aim of all social engineering plots is *gaining trust*. That is why the social engineer is often extremely persuasive, friendly, obliging and always ready to help. After all, people are weak when it comes to answering to someone who is asking for permission politely.

Tips For Employers -- What To Do To Ensure Your Staff Don't Get Fooled

- The employer should make sure all the employees are trained, at least every few months, by a consultant who specializes in security with respect to data breaches and new social engineering approaches.
- The savvy employers should provide employees access to critical data only on a need-to-know basis; plus they should encourage fragmentation of information.
- E-Mail, social networking, instant messaging services could be monitored as confidential data could be easily leaked through e-mails, personal profiles and blogs both intentionally and unintentionally. Product launch dates, products screenshots or branding elements such as logos and boxes are some of the classified types of information that goes public ahead of time.
- Access to the company building should be limited and under the direct supervision of qualified security staff. Imagine this: someone (working for the competition) enters the building, under the pretext that she or he is waiting for someone; but in the meantime, he or she is handing out business cards advertising, in fact, for the competitor.
- Employees should not reveal confidential information over the phone. There are many social engineers who call pretending to be working for a certain company. Moreover they are likely to use a specific lingo familiar to the person receiving the call as they know the company structure and its weak links.
- In big companies, where it is impossible to know everyone, a call coming from a person pretending to be from a certain department can be enough to deceive someone. It is better to check the number before giving sensitive information away. Better still you might even offer to call back. It is known that with colleague-callers rules apply differently and that is why helping a fellow employee with the information he or she needs, can also lead to getting the dirty job done.
- Many times, social engineers will use "emotional" stories to appeal the victim's empathy and inclination to believe in the good faith of his peers. Social engineers may very well take extensive periods of time to know the victims to be in order to study their habits and then serve them exactly the kind of thing that the victims are most likely to fall for: offers of friendship, love, shared interests, lifestyle, and pastime routines. This will create an atmosphere of confidence and the sensitive data will surface.

TipsFor The Employee --What To Do To Prevent Falling For Social Engineering Trickery

- Employees should not share matters related to work, such as campaigns, products, services, complaints, customers with people they do not know or trust. When they need to disclose such information, they should always use the official means of communications between offices (business phone numbers, faxes and e-mail addresses) or discuss it face to face via video-conferencing. Social networking should not be used, unless authorized.
- Employees should not grant access into the building to people who do not work for the company. If outsiders need to enter the office (i.e. for interviews or other business-related purposes), they need to be permanently escorted by an employee.
- Should someone receive a phone call from a person they don't know, who claims to be from another department / office and asks for potentially sensitive data, the best thing would be to tell the caller that they would be phoned back. The employee should call the front desk number and ask to be put through with the person who has called. This way they can check if the person really works there and furthermore if he/she is in the building.
- Employees should be extremely careful when and to whom they need to hand the removable devices, laptops or files that contain confidential data.
- Employees should check twice when it comes to e-mails that come from people asking for confidential data. Double-checking via a phone would also be a good thing as the social engineer can create a site that resembles a legit one in order to launch a phishing attack designed to trick you into willingly providing sensitive data that otherwise you would be against giving away.
- Employees should never perform computer maintenance tasks such as installing patches, hardware (i.e. modems), disabling anti-virus solutions or opening ports as per phone requests. They should always check this kind of requests with the IT department via phone or even better in person.
- All in all, trust can be not only the catalyst of a successful business and of a productive work environment but also the deceiving tool of an intruder who wants to easily get access to critical data and destroy a business. Therefore, it is advisable to handle sensitive data with extreme caution at all times.
- **Research The Facts --** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
- **Slow Down --** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.

And Never Forget, Trust Is Earned

To join the ITSIG, you must first become a member of InfraGard.
To join: **http://www.infragard.net/member.php**

For more information about the MD InfraGard ITSIG or to join, please contact us.

Jim Henderson / CISSP / CCISO
Chairman Of The Maryland Infragard Insider Threat Special Interest Group
Cyber Security-Information Systems Security Program Management Training Course Instructor
Counterespionage Training Course Instructor
561-809-6800
Websites:
www.topsecretprotection.com
www.counterespionage.us
E-Mail:
jimhenderson@counterespionage.us

R.C. Smith
Co-Chair MD InfraGard Insider Threat Special Interest Group
MD InfraGard 2nd Vice President
Lockeed Martin
Industrial Security Manager
7100 Standard Drive
Hanover, MD 21076
W: 410-796-2155
C: 443-690-7710
F: 410-796-7886
robert.c.smith@lmco.com

Disclaimer

The information / content presented in this document is for informational and educational purposes only. Any information / content presented does not imply endorsement by the InfraGard Maryland Members Alliance, Inc. (IMMA) nor by the IMMA Insider Threat Special Interest Group (SIG). Nothing presented in this document, or verbally presented by an IMMA member or IMMA Insider Threat SIG member, should be construed as legal advice or binding.

Products And Manufacturers Referenced

Any products and manufacturers referenced in this document, are for informational purposes only, and do not constitute product approval or endorsement by InfarGard, the Maryland (MD) InfraGard or the MD Insider Threat Special Interest Group.

Legal Advice

Please contact a qualified attorney to interpret any federal or state government laws, regulations, or constructs. Any products or manufacturers referenced are included for informational purposes only, and do not constitute product approval nor endorsement by the IMMA Insider Threat SIG or it members, or any member of IMMA thereto.