# The INFormer—Security Edition

Volume 1, Issue 2 April 2013

INtegrity First Corporation

## Human Error...Impossible to Eliminate

No matter how secure your firewall and virus protection, your company data is ultimately in the hands of your employees. In this month's INFormer, we will discuss different ways that valuable information can be breached due to the one exposure that is unable to be eliminated – ***the human factor***. It is impossible to eliminate all human error even with the best of employees, so preparedness and education, like this newsletter, are great tools against this exposure.

The **best** way to protect your company against this threat is to purchase a privacy/data breach insurance policy. In the event of a data breach, this insurance provides important coverage where your other insurances will not apply. Applying for a quote is simple and quick , all you have to answer is 4 questions! To get a quick quote, call INF or fill out the indication sheet online at: **http://integrityfirstins.biz/Home/CyberIndicationForm**

## Phishing for Information – Don't be the "Catch of the Day"

Phishing, a form of social engineering, is what happens when a fraudulent email is sent out that appears to be from a legitimate source and asks for some piece of personal information, such as a username/password combination. These emails will often appear to be from a trusted source. The email will either ask for information to be sent back, will take the user to a site which looks and acts very similar to the trusted source's site, or will install malware when links in the email are clicked on.

In a recent survey, 87% of people said that they would be able to identify a phishing scheme…61% failed. As technology becomes a bigger part of our lives, phishing has moved from emails to text messages and social media posts!

To protect yourself and your company from these schemes, adhere to the following rules:

*Never put personal information into a pop-up window from an email:* This is a common trick used by "phishers". The pop-up will look like a legitimate site, but it will not be. Type the known, safe address into your browser instead of following the link.

*Verify that the web address begins with "https://" when entering personally identifiable information:* This is one sign that the site is secure because all of the data sent back and forth from the server is encrypted using SSL (Secure Sockets Layer).

*Don't click on links in emails from people you don't trust:* Links can have malware and viruses associated with them, so it is a good idea to never click on a link in an email from an unknown entity.

*Keep your security software up to date:* This is the easiest way to protect yourself and your company. Schedule updates to be installed automatically every night on your computer. This way, you will never be more than 24 hours out of date.

*Don't reply to an email with any personal information, such as a credit card number or a social security number:* There are rules in place which do not allow companies to ask you for your information in this way. If you get an email from a company asking for personal information, call the company right away. They will need to know that they are being used in a phishing scheme.

If you do receive a phishing email, be sure to report it to:

**reportphishing@antiphishing.org**

They are the Anti-Phishing Working Action Group and will take the appropriate action on the scheme.

### Inside this issue:



### Special points of interest:

- ⇒ Learn the best ways to protect your company from phishing schemes
- ⇒ Learn where to report phishing schemes
- ⇒ Look for seven commonly used social engineering tactic
- ⇒ Secure-A-Day is offered by INF to advise on security risks

Get the electronic version of this newsletter at: http://integrityfirstins.biz/Content/Security-INFormer1-2.pdf


INtegrity First Corporation

3633 Poplar Avenue
Pittsburgh, PA 15234

Phone: 412.563.2106
Fax: 412.563.6109
Email: info@integrityfirstins.biz
Web: www.integrityfirstins.biz


This quarterly newsletter is created by Stacey Ivol. Stacey has her Bachelor of Engineering degree from the University of South Carolina in Computer Engineering as well as her Masters of Science degree from Carnegie-Mellon University in Computer Engineering, with a focus on cryptography. She is the Vice President of the Privacy/Data Breach Unit for INF, Web Master for multiple companies and does security consulting for small businesses. She also teaches the Secure-A-Day class for INF.

Secure-A-Day is offered by INF to review security exposures commonly encountered throughout a typical workday and ways to mitigate them. For more information on this class, visit: http://integrityfirstins.biz/Home/SecureADayDetails or call INF!

# Social Engineering – What it is and How to Avoid it

Social Engineering is the art of retrieving information by manipulating people. Social engineering can come in many forms and accounts for about 10% of the data breaches that have taken place in the past year. Social engineers will do whatever it takes to gain trust and exploit that trust whenever possible. They rely on the fact that people want to be helpful in general. Common social engineering tactics include:

*Wearing a third-party vendor uniform:* Most people automatically assume that the uniform gives a person credibility. This is not the case. Most vendors require their employees to have company badges, which can be forged. The best way to verify the identity of the vendor employee is to call the vendor and verify multiple things about the employee. Some people may believe that this is going overboard, but most vendors have access to an entire office, so a two-minute phone call should be a small burden to protect the safety of your data.

*Shoulder Surfing:* Social engineers have perfected the art of cruising by you at the local Starbucks or Barnes and Noble and watching you type in your password. Don't make it easy on them and make sure that you always have "Hide Password" checked anywhere you enter passwords, which will make the letters show up as dots. Additionally, try to make sure that you are angled in such a way that it would be difficult for someone to see what you are typing.

*Dumpster Diving:* Trash outside a company is valuable! Most employees do not realize the value of their trash. Org charts, internal phone numbers, and client lists are just a few of very valuable pieces of information that a social engineer will exploit from the trash. When in doubt, shred your trash with a cross-cut shredder.

*Phone Number Spoofs:* Some social engineers have the ability to make their number show up as a different one on the caller ID, thus allowing them to pretend to be calling from anywhere that you trust. They will normally ask for passwords or credit card numbers, then use that information to benefit themselves. Your caller ID can be manipulated. Never give out personally identifiable information over the phone.

*Piggybacking:* This can also be called shadowing and it happens most in the mornings. A social engineer will appeal to your humane side, asking to borrow your badge because she or he "forgot" it or they will follow you through security and hopefully will not be noticed. This happens during "smoke breaks" as well when people are returning to the office.

*Acting as the Help Desk:* This tactic can happen the most at larger companies with a big IT department. A social engineer will call as the "help desk" and tell an employee that they have been having some issues with the passwords and that the employee needs to change it and let the help desk know what it is. Most people do not think twice about giving the help desk information and the social engineer has successfully gotten the employee's new password.

*Neuro-linguistic Programming:* This is a tactic that must be practiced, but once mastered, is quite effective. A social engineer will mirror your actions, match your voice tone and breathing, and use general mimicry of you to gain your trust in hopes that you divulge personal information that she or he can use.

A company's data is only as secure as the employees keep it. Employee education and having security procedures in place that are reviewed regularly will help a company to avoid the most common social engineering tactics. Even a small company should have security procedures in place so that the employees and employers each know what is expected of the other and how certain situations should be handled. If you do not have a security procedure in place and would like an example, please contact sivol@integrityfirstins.biz.