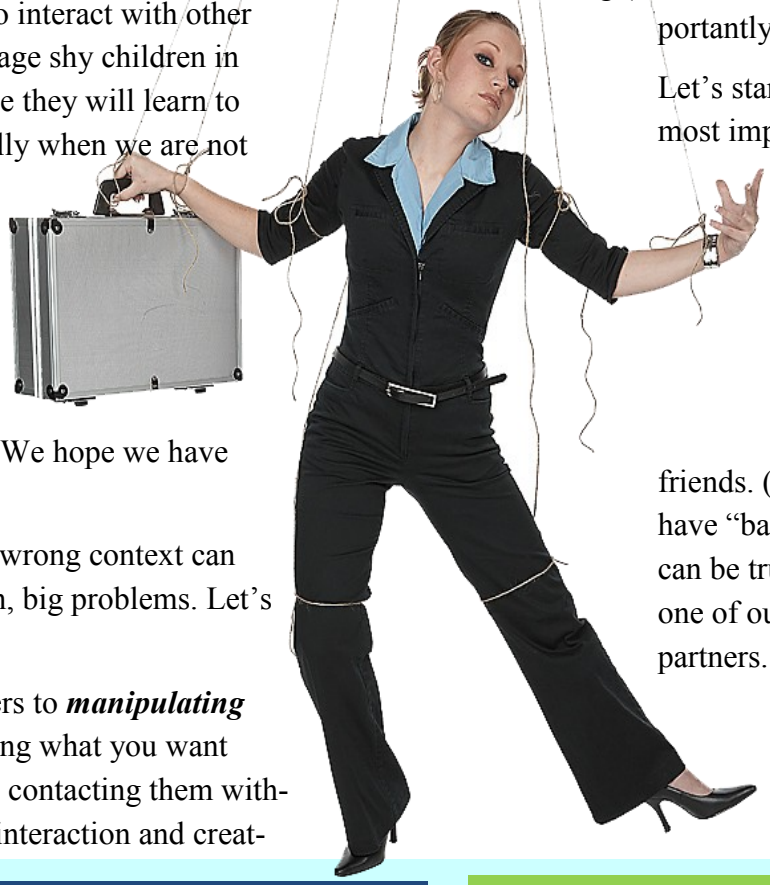
SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter
your energy partner®
OPPD
Omaha Public Power District

Social Engineering
What's So Bad About Being Social?

What's so bad about being social? Well, nothing, actually. Early on we try to teach our children about being friendly. Parents set up play dates to help children learn to interact with other kids. We try to encourage shy children in social settings. We hope they will learn to function conversationally when we are not around. Most importantly, we try to balance their newly acquired social skills with a healthy self-protective skepticism. We hope we have done enough.



Being too social in the wrong context can cause problems, though, big problems. Let's look closer at this.

Social engineering refers to ***manipulating*** another person into doing what you want them to do. It involves contacting them within some kind of social interaction and creating a level of trust with them. So, this kind of manipulation involves communication, a social setting (often on a computer) and most importantly, some level of trust.

Let's start with trust, since that's the most important characteristic of social engineering. The first step for the "social engineer" occurs when they can find an inroad that allows them to communicate with us. Maybe they let us know we have mutual friends. (Read: *my* friends wouldn't have "bad" friends, so maybe they can be trusted.) Perhaps they work at one of our well-respected business partners. (X Company wouldn't have sleazy people working for them, maybe we can trust

Continued on page 4

How Do I Protect My Smart Phone?

Basic Security

Download an antivirus application directly to your smartphone.

Make sure that you always choose a mobile phone from a recognized brand. The phone should come with an IMEI number (see sidebar on page 2).

Scan your device after you download your anti-

Continued on page 2

40% of us would rather lose their wallets than their mobile phones. Yet, most of us do not secure our mobile devices.

McAfee

How Do I Protect My Smart Phone? - continued from page 1

virus application. Set a reminder on your phone to scan periodically, OR , if your antivirus application allows it, set your AV protection to automatically run scans.

Turn off Bluetooth if it is enabled, especially if you are in public access areas.

Protecting your mobile device doesn't differ greatly from the things you should already be doing on your main computer. For example, don't click on unfamiliar links, don't reply to or even open messages from unknown senders. Assume all Wi-Fi hotspots have no security, keep your systems up-to-date. The same warnings apply for both mobile security and computer security. Following these rules will minimize your mobile risk.

Additionally, you might want to consider these points when using your smart phone.

- Avoid downloading unknown software from the Internet. That sounds obvious, but the fact remains that lots of bad things can "tag along" with the apps you may want for your phone. When you want to download a mobile app, make sure it's from a reliable source.
- Make a backup of your contact list. Early examples of people losing their phones should have taught this lesson, but hearing the warning again might spur user action.
- Before you accept any multi-media content, be certain you know the source.
- If you have Bluetooth, set the option for the undiscoverable mode. Never accept data from sources you do not know and trust.
- Your smart phone has a password. Using it will help protect the data you own and walk around with.
- Before you accept any multi-media content, be certain you know the source.
- If you have Bluetooth, set the option for the undiscoverable mode. Never accept data from sources you do not know and trust.
- Your smart phone has a password. Using it will help protect the data you own and carry with you.

IMEI

(International Mobile Station Equipment Identification)

That's the serial number associated with most mobile and satellite phones. Most often, manufacturers put this number inside the battery compartment of the phone or with the system information on the settings menu. Some phones allow it to be displayed when you type *#06# on the dialing pad.

You can effectively turn off the phone service for a stolen phone in many cases by reporting this number to your service provider.

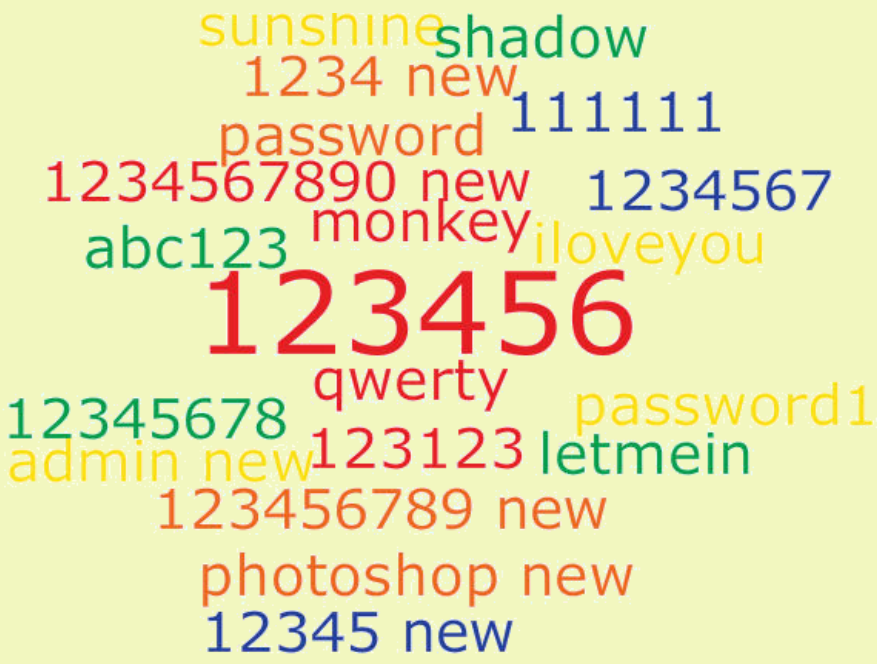
PASSWORDS—AGAIN?

YOU'RE KIDDING, RIGHT?

Well, it can't possibly be anyone from OPPD, but people do exist, somewhere, who still use passwords as bad as those listed in the word cloud below. (If you recognize one of the passwords as yours, I suggest you stop reading RIGHT NOW and change it!) In fact, according to reports published by SplashData, for the first time since they started tracking, *password* lost it's top spot as the worst of all passwords. *123456* replaced it as the worst possible password in 2013.

New passwords to the 2013 list include, *1234, 1234567890, 123456789, 12345* and *photoshop*. (Adobe experienced a security breach in 2013, causing some not-very-creative users to use *photoshop* as a password, and the others are, well, just examples of laziness.)

Looking at the list, a couple of things should be apparent to you. Only **one** of these easily-guessed passwords uses a combination of letters and numbers, *abc123*. (That one probably belongs to those users either obsessed with early Michael Jackson songs or those who might be just learning their letters, ahem.) A good password uses a combination of three different types of characters such as, letters, numbers, capitalizations or symbols.



The number strings, *iloveyou, letmein,* and *qwerty* aside, the rest are real words. Hackers often use programs that run through the dictionary to guess passwords, which explains why experts recommend **not** using real words as passwords, unless you add numbers, capitalize random letters or add symbols somewhere.

And then there are the number strings. Yikes! Not only are they in series format, they all start with *1*. Not one even bothers to reverse the order, skip numbers in the series or duplicate any numbers!

Perhaps with more and more security breaches reported, users will start to take password security seriously. If not, maybe next year your guessable password will be at the top of the "worst" list.

What criteria does SplashData use to compile this list? Well, it compiles this ignominious list from a database of stolen passwords posted online.

Social Engineering—What's So Bad About Being Social? Continued from page 1

them.) This mentality allows Facebook and Linked-In to connect people with each other. But, what happened to the healthy skepticism you learned earlier in life? You don't really know your friend's friends, but you've extended your trust anyway.

Now that your guard is down, since you "pseudo know" this person, they move on to the next step. This happens when, as good con artists, they trick you into disclosing information they need. Maybe they need your mother's maiden name. They trick you into disclosing this during a discussion about people's crazy relatives. Maybe they talk about your favorite sports team, and share a link to their fantasy site, which happens to have key-logging software loaded into it. There are plenty of seemingly friendly, non-threatening ways they ***manipulate*** you into disclosing information to them. They never ask direct questions. The social engineers realize that asking a direct question will raise your guard. That would seem nosy, after all. They just chat with you, a much easier way to get you to inadvertently disclose information. Once armed with your information, they may access your personal accounts or they may use your Facebook, Twitter or Linked-In account to "reach-out" to more of your unsuspecting friends using your identity. They may even start sending you targeted emails, all of which contain links to malware sites.

Ironically, once again, we are our own worst enemy. Bottom line here. Would you accept a "gift" from a stranger you just met on the street. Would you take their directions to find something special at a location you don't recognize? Would you share your personal history, family information, or job information with this person? You would certainly warn your kids away from doing any of the above things.

Why is it different for you?

OUR MOTHERS

THE ORIGINAL SOCIAL ENGINEERS

I can hear the laughing from here. You think I jest? Think about this. If my mother knew the last name of a friend, the next set of comments would have to do with people she knows with the same last name. "I wonder if they may be related to so-and-so." Anything you **utter** would either confirm or deny the relation, so unless you remain mute, you've answered the question. Giving up the last name opened up the floodgates of information for her.

Like all good detectives, my Irish Catholic mother had a great knack for finding out things without directly asking. My mom's best innocent-sounding question was "What parish is so-and-so from?" Of course, any parish named gave her the answer to "Is this person Catholic?" and "Where do they live?" Answering with a non-Catholic church revealed the denomination of the individual, presumably active in their church otherwise it would not be mentioned conversationally, and where they lived. Knowing where someone lives reveals a lot of information in itself.

It's the same way today. Your name, where you live, who you know, where you went to school, who you're related to, all reveal things that social engineers can use to "pretend-to--know" you and get information from you. Stop and think about what your innocent comments give away about you, before you open the information floodgates.

North American Electric Reliability Corporation (NERC)

Quarterly Update

As NERC Cyber Infrastructure Protection (CIP) version five requirements are being finalized and as entities are preparing for the April 1, 2016 compliance deadline to approach, CIP impacted companies and personnel must not forget the requirements for CIP version three are still active and enforceable. With that said OPPD's NERC CIP access process for employees and contractors is this quarter's topic of discussion.

OPPD employees and vendor supporting services personnel requesting authorized non-escorted physical access and/ or authorized cyber access to Critical Cyber Assets must submit an access request form (electronic or hardcopy) and complete the following requirements prior to access activation:

Cyber Security Training (CST) – Per CIP004-3, R2 CST is mandatory for all employees and contractors that work within any OPPD dedicated NERC location. CST can be administered either on-site or prior to the contractor's arrival. Training must be completed prior to allowing unescorted access.

Personnel Risk Assessment (PRA) –Per NERC CIP004 -3 R3, prior to responsible entities shall ensure that each assessment conducted include, at least, identity verification (e.g., SSN, State ID, DL) and a seven year criminal check. PRAs (background checks) must be completed prior to allowing unescorted access.

OPPD Employees can submit access requests via OPPD's CIP Pending application which is OPPD's automated NERC CIP Access request application. OPPD's CIP Pending application has been designed to assist those employees who currently do not have NERC CIP access or employees requesting additional NERC CIP access permissions. Managers and/ or Supervisors of requesting personnel must submit the access request on behalf of the OPPD employee.

OPPD contractors requiring access within OPPD NERC CIP Facilities must continue to work with your OPPD sponsor. OPPD NERC CIP Access forms (Paper) are still to be utilized for OPPD contracted personnel and shall be filled out the OPPD sponsor. Authorization for such access is routed and reviewed in accordance to the authorization list located at the bottom of the form. Training and Background Checks are completed by OPPD's Reliability Compliance and Transmission Services department and OPPD's Corporate Security Department. Authorized non-escorted physical access and/ or authorized cyber access to Critical Cyber Assets shall be granted upon the completion of all requirements.

Also, just as a reminder to all OPPD vendor supporting services:

NERC CIP standards also require contractors/ vendors with unescorted access to secure areas to have access removed within 24 hours when that individual no longer needs access, which includes the termination of said employee/contractor. As noted within your Terms and Conditions within your contract, every contractor is required to notify OPPD (Central Security @ 402-636-3700) within two hours of an employee not requiring unescorted access and/or an employee being terminated from his/her job. Failure to do so may result in breach of contract. Contractor badges must be returned to your sponsor or to the following address:

OPPD
Attn: Rod Rodgers 5E/EP2
444 South 16th St.
Omaha, NE. 68102

For more information pertaining to OPPD's NERC CIP Access requirement please contact Mike Nickels - OPPD Reliability Compliance Specialist manickels@oppd.com, (402) 552-5036.