The DynaSis Education Series for C-Level Executives

Employee Training as a Tool for Cyber Security

Many data breaches caused by employee negligence.

In a recent survey of more than 600 Internet security professionals at enterprise level businesses, two-thirds of them agreed that their own employees were the weakest link in establishing and maintaining a strong security environment. In fact, another survey showed that more than 50% of companies surveyed were able to link a security incident to a careless or untrained employee. Only 35% of the 600+ security professionals in the first survey believed that senior company executives prioritized data security and how it might affect their companies, and 60% felt that employees had little or no real knowledge of the cyber risks their employers face.

According to Michael Bruemer, a VP with Experian Data Breach Resolution, *"It's no surprise that employee-related security risk is their number one concern. As we have seen in our incident response service that we do for clients, about 80% of all the breaches we service have a root cause in some type of employee negligence."* **80%!**

So we ask: if this is the current situation at enterprise level businesses, businesses that can afford full-time cyber security professionals, where does this leave the small to midsized company? Add to this the reality that today, in spite of the headlines about major breaches at large well-known companies, the vast majority of cyber attacks are, in fact, against the small to mid-sized business.

It's no secret that the Internet has provided us, and our employees, with many advantages, from ordering pizza for an employee lunch, to researching products and services our business needs to function better, to researching the competition, to instant banking, etc., etc. But any of these actions can inadvertently cause a company great harm, even bring it down, if we do not employ the correct security measures, and one of these measures is employee training. Below are a number of areas that require training of company employees:

Passwords

As simple as it may sound, and we know you have heard it again and again, one of your best defenses is the use of strong passwords. This is truly your first line of defense against cyber attacks, but, unfortunately, this admonition all too often falls on deaf ears. Birthdays, pet's names, favorite song titles…not good ideas. Most people have now gone past the idea of using "Password" as their password, or "1234ABC", but here are some tips to pass on to your employees on how to create passwords that are truly difficult to break.

1: Use at least eight characters, including upper and lower case letters, number and symbols. If you have created an online password recently for a shopping site such as Amazon or a department store, virtually all of these have gone to this methodology and require this type of password for access. There is a reason for this: it works!

2: Make the passwords cryptic, hard to figure out. But also make sure you can remember them. bBall!!3102 works for a basketball fan who had an important event happen…but not a birthday…in 2013 (backwards in the password).

3: Do not use personal information. This includes your name or family or pet's names, in any form, or your company's name. Encrypted dates can work, but not those that can be traced back to you, such as birthdays, wedding anniversaries, employment dates, etc. Do you remember the year you went to your first rock concert? 1992 can become 2991, 1929, 1299, etc.

4: Passwords should be treated as very personal information, not to be shared with anyone. Not with family, friends or co-workers. If you absolutely must share a password with someone, change it immediately. Your co-worker may not have any malicious intent, but he may also not be as diligent about protecting passwords as you and you don't want to be caught up in a mess someone else creates. In fact, it's far better to prevent the mess from ever occurring.

5: As annoying as this may be, you should have different passwords for every account, particularly those relating to money or highly sensitive information. If you use the same password, when someone gains access to one of your accounts, they have access to all of them.

As an employer, you should also consider either enforcing a policy requiring that passwords be changed every 90 days, or speak with your IT service provider about installing a multi-factor password protection system such as Kasaya's AuthAnvil. An application such as this can be cost effective and make it much easier for your people to effectively use passwords securely.

Use of Unauthorized Software

There are a great many software programs available today by simply clicking a button and downloading them. Many are free. Many provide great tools to simplify and speed up a project. Many also contain an incredible variety of malware, ransom ware and viruses that can sit quietly while sending data back to the cybercriminal who planted it there, or totally lock your system until you pay a "ransom" for the key to unlock it. The rule should be very simple: if the company didn't provide it, you don't use it. If an employee finds online software he/she wants to use, this product must be cleared by the company's in-house IT professional or its managed IT service provider before it is used.

Social Engineering or "Phishing"

Social Engineering is a criminal tactic in which people are manipulated into parting with confidential information. Today we laugh when we receive an email from our friend the Nigerian Prince who seeks our help in hiding his $200,000,000 fortune in the US and for your brief assistance will gladly pay you a paltry fee in the amount of $5,000,000 as long as you provide the $3,000 in U.S. funds he needs to wire the funds across the Atlantic. But will you laugh when that email seems like it is coming from Wells Fargo, Citibank, Chase or whichever bank is yours? Or if that email is from the IRS? (As an aside, the IRS NEVER sends emails, NEVER calls. If they want to contact you, they send a notification through the US Mail. And they send it twice.)

Psychologists will tell you that most people, not all, have a natural inclination to trust, and convincing you to eagerly give up your information is a lot easier than hacking a well thought out password. Of all the ways the cyber criminal can steal your information, the weakest link in cyber security is the person who trusts emails that look right, but in reality come from wrong sources. A bank will not send an email to reset your password. The cyber criminal fools you into giving up your current password in the fraudulent reset process, and before you discover what has happened, has drained your account, transferring your money to an offshore bank. Similarly, the IRS is not going to send you an email asking for your social security number. They already know your social security number!

These are obvious situations, but (fake) department stores, (fake) loan companies, (fake) credit bureaus, and others can be just as dangerous. You may ask: how do they know I bank at Wells Fargo? Answer: they don't. But if they send out a million fraudulent emails, some of those recipients will actually be Wells Fargo customers, and a few of those will fall for their scheme. That's all they are looking for.

Another common attack is to receive an email from a friend. The perpetrator hacks your email account, downloads your contacts, and in minutes everyone you know is receiving emails "from you," asking for a donation to a non-existent charity, or seeking personal information.

All these scenarios are important parts of employee training. An attack can be against the employee personally, or against the employee with the goal being an attack against your company.

Social Media Scams

Not surprisingly, the explosive growth of social media has lead to an explosion of scams targeting those who use and enjoy social media, and as business centric social media grows, so do the scams aimed at employees as a way to exploit their employers. Here some of the most recent, most successful…but please don't think this is a complete list:

1: Using Twitter to set up fake customer service accounts

Cyber criminals set up accounts that look like the legitimate customer service accounts of real businesses except that a single, obscure character may be off, like an extra underscore, or transposed letters. People make mistakes when typing, especially on smartphone virtual keyboards. Experience has shown us that if 10,000 people search for AbcXyz company, a certain small percentage will mistype and end up with AcbXyz, or AbcXzy, or Abc Xyz. By creating hundreds

of these "error" accounts, the thief will trap a number of people, some of whom will fall for the scam.

2: Posting fake comments

Adding fake comments to popular posts intending to draw other comments so they can discern email information, which often leads to fake credit card phishing scams, among others.

3: Faking live-streamed videos

Again, posting comments to streamed videos can lead to links to fake websites that offer free live streaming of a game or event, only to find that these links lead to sites that ask for the visitor's personal info in order to gain access…but there is no actual streaming available.

4: Criminals set up fake social media accounts for companies like NetFlix, pretending to offer real promotions. Of course, they require personal information…and, of course, there is no promotion just a scammer after your money.

5: Online surveys and fake contests

The basic concept is not new; companies have been setting up surveys and contests for years, collecting information and then selling it. Legitimate companies use this information legitimately, even if it is annoying, but fraudsters use it to gain access to personal and business accounts.

As an employer, keep in mind that every one of the illicit tactics mentioned throughout paper can be used against companies as well as individuals. Remember, companies are made up of individuals.

So how do you institute good security habits in your company? Follow this plan:

1: Lead by example. It has to start at the top. If the boss (owner, president, department manager, etc.), doesn't follow good practices, can you expect anyone else to? Are your passwords taped to your computer? Is your unlocked laptop left in the conference room overnight?

2: Provide daily tips on security. No one is going to read that 100 page manual on security. Not even you. But little tidbits of information that can be easily absorbed can be very effective. Make it interesting. It should not end up just being a list of "don'ts". Educate people. Explain what's going on out there. Define "phishing", "ransomware", and other terms.

3: Once you create your security polices, enforce them! Enterprise level companies often have "security police" who can effectively monitor the effectiveness of such policies. Small to mid-sized businesses are more inclined to enforce at the beginning, then let these policies slip over time.

4: Putting people to the test. Creating policies and educating people will only go so far. Think about real-world simulations. You can either bring in a cyber-security expert or do this in-house. Test employees who actually have access to the sensitive data you are trying to protect. Try and

coerce them into parting with the same information that a cyber thief would be after. If they crack, it doesn't mean they are bad employees; it means you need to provide more training.

5: Provide security tools and make them easily accessible. You can have the world's best security tools – data encryption, VPNs, malware scanners – but don't expect wide usage unless they are easy to use. It's like the paper shredder: you may have a world-class device to destroy sensitive paper documents, but if it is located on the far side of the office, the discards are probably going to go into the waste-basket instead.

As a managed IT service provider serving hundreds of small to midsized businesses throughout the Atlanta metro area, we at DynaSis fully understand the incredible creativity of today's cyber-criminal. We also understand that staying out on front of the situation is a full-time job and training employees is part of that job. Please feel free to call us at 678.373.0716 if you have any questions.

https://staysafeonline.org/business-safe-online/train-your-employees

https://www.sophos.com/en-us/security-news-trends/it-security-dos-and-donts.aspx

http://www.tripwire.com/state-of-security/security-awareness/8-security-practices-to-use-in-your-employee-training-and-awareness-program/

https://www.travelers.com/resources/cyber-security/cyber-security-training-for-employees.aspx

http://www.pcworld.com/article/2861031/how-to-train-your-staff-on-cyber-security-and-make-it-stick.html

http://www.darkreading.com/vulnerabilities---threats/employee-negligence-the-cause-of-many-data-breaches-/d/d-id/1325656

https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering