IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

Inside This Month's Newsletter

JULY 2016

This monthly publication provided courtesy of Howard Globus, Security Evangelist & Partner of **IT On Demand.**

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

5 Ways To Spot A Social Engineering Attack

"I'm not going to make payroll – we're going to close our doors as a result of the fraud."

Unfortunately, that statement is becoming more common among smaller businesses, according to Mitchell Thompson, head of an FBI financial cybercrimes task force in New York.

The FBI reports that since October 2013 more than 12,000 businesses worldwide have been targeted by social engineering–type cyberscams, netting criminals well over $2 billion. And those are just the reported cases. Often, due to customer relationships, PR or other concerns, incidents go unreported.

These unfortunate events were triggered by a particularly nasty form of cyberattack known as "social engineering."

Social engineering is a method cyber con artists use to lure well-meaning individuals into breaking normal security procedures. They appeal to vanity, authority or greed to exploit their victims. Even a simple willingness to help can be used to extract sensitive data. An attacker might pose as a coworker with an urgent problem that requires otherwise off-limits network resources, for example.

They can be devastatingly effective, and outrageously difficult to defend against.

The key to shielding your network from this threat is a keen, ongoing awareness throughout your organization. To nip one of these scams in the bud, every member of your team must remain alert to these five telltale tactics:

2. **Baiting** – In baiting, the attacker dangles something enticing to move his victim to action. It could be a movie or music download. Or something like a USB flash drive with company logo, labeled "Executive Salary Summary 2016 Q1," left where a victim can easily find it. Once these files are downloaded, or the USB drive is plugged in, the person's or company's computer is infected, providing a point of access for the criminal. **Phishing** – Phishing employs a fake e-mail, chat or website that appears legit. It may convey a message from a bank or

Continued on page 2

other well-known entity asking to "verify" login information. Another ploy is a hacker conveying a well-disguised message claiming you are the "winner" of some prize, along with a request for banking information. Others even appear to be a plea from some charity following a natural disaster. And, unfortunately for the naive, these schemes can be insidiously effective.

"It's critical to keep your network patched, secure and up-to-date."

3. **Pretexting** – Pretexting is the human version of phishing, where someone impersonates a trusted individual or authority figure to gain access to login details. It could be a fake IT support person supposedly needing to do maintenance…or an investigator performing a company audit. Other trusted roles might include police officer, tax authority or even custodial personnel, faking an identity to break into your network.
4. **Quid Pro Quo** – A con artist may offer to swap some nifty little goody for information… It could be a t-shirt, or access to an online game or service in exchange for login credentials. Or it could be a researcher asking for your password as part of an experiment with a $100 reward for completion. If it seems fishy, or just a little too good to be true, proceed with extreme caution, or just exit out.
5. **Tailgating** – When somebody follows you into a restricted area, physical or online, you may be dealing with a tailgater. For instance, a legit-looking person may ask you to hold open the door behind you because they forgot their company RFID card. Or someone asks to borrow your laptop or computer to perform a simple task, when in reality they are installing malware.

The problem with social engineering attacks is you can't easily protect your network against them with a simple software or hardware fix. Your whole organization needs to be trained, alert and vigilant against this kind of incursion.

For more on social engineering as well as other similar cyberthreats you need to protect your network from, get our latest special report on this crucial topic:

The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind

Don't let your organization be caught like a sitting duck! You've worked way too hard to get where you are today to risk it all due to some little cyberhack you didn't know about. Call us at (212)235-0260 or complete the form at www.it-on-demand.com/hackers-10/ and get your copy of this crucial preventive guide today – before your company becomes yet another social engineering statistic.

See What Our Clients Are Saying...

"Howard Globus & IT On Demand are excellent! My critical files are backed up automatically every 15 minutes. Each quarter they call me to perform a test recover, so we know my files will be accessible when I need them in a crisis. I've referred IT On Demand many times and I recommend them without qualification!"

–Tony Martignetti Esq., Martignetti Planned Giving Advisors, LLC

"The International Advertising Association operates globally across all time zones. We need reliable, knowledgeable and responsive IT support – without the burden of on-staff resources or expense. Right from the start IT On Demand has provided us with an impressive level of 24/7 service and reliability. They understand our operations. And they ensure that our IT assets operate and function optimally."

–Michael Lee, International Advertising Association

Tips For Securing A New Business

Establishing a new business is an exciting time! You get to decide the name, the logos and designs you'll implement, what you'll be selling or offering your customers, etc. Designing the office or store space is something to look forward to and hiring your first staff members is a thrill! Where does cyber security fit into your plan? Have you thought about it? Come up with a strategy? While deciding on how best to implement cyber security for your business may not be as engaging as creating the rest of your business plan, it is one of the more important components that needs your time and energy.

Developing a strategic internet security plan while you're designing and launching your new business will be most effective from the start. When considering the cyber security plan for your business, here are some tips to keep in mind to minimize potential threats to your business.

When it comes to your finances, share the wealth! While keeping all things money with the same bank may seem like the easiest way to do business, think about how devastating it would be should a person get their hands on your account information. When a hacker attacks, this is exactly the information they are looking for. By splitting the finances for your business into separate accounts, it will be more difficult for someone to find the account numbers and codes for each account. Depending on how you structure your business, different employees could have access to different accounts, keeping the knowledge separate. Have a separate account for all operating capital, one that only you have access to.

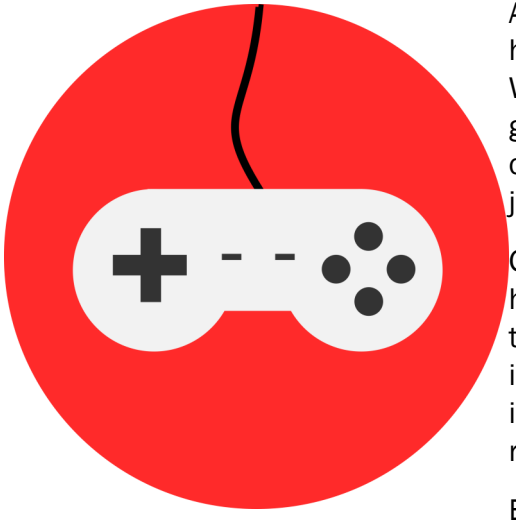
In the wake of identity theft and businesses suffering from hackers, credit monitoring services have grown in popularity. A credit monitoring service charges a monthly fee to keep an eye on your credit and see if any credit lines have been opened in your name that you did not apply for. As a business owner, you'll be a more likely target for those searching to do just that - open a bunch of lines of credit in your name, steal your finances, and have the time of their life! Since credit monitoring only alerts you to activity, a better option is to freeze your credit. By freezing your credit, you prevent anyone from being able to come in and steal your money or financial information. Freezing your credit costs a mere 10.00 to do and you'll be better protected from those who wish to steal your information.

Our last tip for new business owners is to spend some time deciding on what customer information is really needed and for how long it will be kept. Think about all of the services you joined, organizations you signed up for, and stores you've shopped at. How many times have you been filling out a form and thought to yourself, "Why do they need to know that?" Ask yourself the same question. Why do you need to know this about your customers? Collecting only imperative data and storing it for the shortest amount of time possible is best practice for businesses. In the event of a security breach, a percentage of customers would be affected instead of any customer you've ever had if you stored information indefinitely. Storing data on removable devices is a great option as well. If it's not online, it's not able to be stolen!

For the best protection of your new business, creating a strategy plan from the beginning is your best bet. Cyber security needs to be a priority. While there are countless steps you can take to protect yourself and your business, the three tips above are a great starting point. Call us at **(212) 235-0260** and we will be glad to meet with you and discuss our recommendations. In fact, to the **first 3 companies** that contact us before **August 5th,** IT On Demand will provide a FREE Security Assessment, which will determine where your vulnerabilities are and how to minimize your risks! Call us to request your free assessment today!

**Offer valid to qualified prospective clients with 10 or more computers and a minimum of 1 server.*

The "Game" of CyberSecurity



As a kid, who among us did not dream of being paid to play games? To have an adult life that was every bit as stimulating as our childhood? While the lucky ones have managed to make a living and a career of game playing, for the majority, it just isn't happening. But now with the concept of gamification, cyber-security for your business and employees just got a whole lot more fun!

Gamification is a method used to help employees adopt and make a habit of best practices in cyber-security. It engages those who use it by taking the mechanics of gaming, the fun parts, and implementing them in non-gaming situations, which are not so fun. Gamification takes the idea from games that with good play comes reward. When people are rewarded for doing their best in any situation, they are driven to do so.

By rewarding good behavior with something like collectible badges or tickets, employees will be more apt to try to earn them. For example, when an employee sends so many emails without a red flag, they might earn a ticket. When they have collected a preset number of tickets, they can earn a tangible reward like a gift card or maybe extra time off. For those employees who continue to ignore best cyber practices, you could set up notification that triggers an alert of those who need further training.

While the concept of gamification seems incredibly simple, and it is, it can save you a lot of time, effort, and money in training. When a training schedule is conceived, it looks fantastic on paper. All employees will attend so many sessions and put into practice what they learned, right? Wrong. We know that this is rarely the case. By utilizing gamification, you can weed out who knows what they're doing from those who don't and focus additional training sessions with only the people who need it. You save time and money and the employees who get it are allowed to keep working.

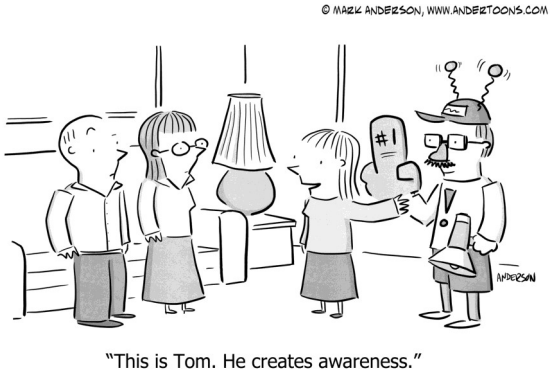
Encouraging employees to share their successes by keeping track of rewards earned will increase buy in to the training regiment. People want to be recognized. They want to show off how well they're doing. You can foster an environment of friendly competition, further increasing participation and long-term behavior change when it comes to safe cyber use. By starting regular audits of how secure your business, you will have the data you need to change up gamification training to suit your needs at any given time.

Gamification is a way to take the idea of behavior modification through rewards and apply it to a real life, professional, business setting. Your employees could gain the skills they need for safe cyber use in a fun, appealing way and cyber security for your business will increase. It is possibly a technique that would make both parties happy! It's a textbook win-win situation!

Favorite Quote of the Month:

"Darkness cannot drive out darkness; only light can do that. Hate cannot drive out hate; only love can do that."

-- Martin Luther King, Jr.



"This is Tom. He creates awareness."