THE NAVIGATOR
COMPASS
NETWORK GROUP

FEBRUARY 2016

In this issue...

Spear Phishing: The Cyber Threat on Every Business Owner's Mind

wk1003mike / Shutterstock.com

Spear phishing, or malicious emails targeted at specific industries, businesses, or individuals, is a top security concern amongst many American business owners.

The average cost for a US business when they are successfully attacked by a spear phishing campaign is $1.8 million, and many security firms and solutions providers say these highly targeted email pushes are responsible for a great majority of security incidents. But why is this? Why are individuals so easily swayed to drop security protocols because of a simple message?

This level of temptation is induced by the targeted nature of the attack. If the attacker's techniques are sophisticated, the email nearly forces an individual to click a link or download an attachment within the message. This form of cyber threats uses manipulative tactics to wrongfully take login credentials or to install malware on a victim's workstation to access mission-critical data and private information. Because the content inside these emails are very specific to the victim, it's more believable and, oftentimes, the credibility of the message isn't even considered.

To security companies, spear phishing is a huge concern because it exploits the vulnerabilities in people as opposed to the vulnerabilities in technology. This means that if a malicious email gets past their spam filters (which does happen), then the security of their client's data is out of their hands. At this point, the company's only defense is their staff members. Are you and your coworkers able to detect and avoid these highly sophisticated and targeted emails? Let's hope so.

Here are a few quick tips, in the form of questions, to help you better detect and avoid spear phishing:

1. Who is the sender? Do you know this individual personally? If it's from a well-known company, is the company name, logo, and contact information represented correctly?
2. What is the email asking you to do? Do companies normally ask people to do this type of action over the internet or through email communication? For example: Your bank is asking you to update your login credentials. In your experience, an update would be requested when you're on the website attempting to login, and it wouldn't normally be requested through email. So, to verify this type of email, you can exit out of the email and visit the website manually by typing the known URL into the address bar (not the URL provided in the link), or you can call the company (with contact information provided on their website, not in the email) and verify the request with a representative.
3. Is there an attachment? If so, do you know who the sender is personally? If not, what is the intent of the download and why is it absolutely necessary for you to download it? Never download an attachment from an unknown source without first verifying the sender. For example: Jane Doe from XYZ Company sends you an email with an attachment. You currently do business with this company, and she references your position and is aware of your job duties (making the email legitimate and targeted). However, you don't know who Jane Doe is, and you're not sure why she'd be contacting you (making the email "phishy"). To verify the sender, call XYZ Company with the contact information you have (not the information she supplied you with) and ask to speak directly with Jane Doe. If no one there knows of a Jane Doe, then you should immediately delete the email and notify your security provider. If she answers and explains the intent of the email, then you can (most likely) safely open the email.

If you have any further questions regarding Spear Phishing and the threat it poses to your business, then give us a call today. We'd be happy to answer any of your questions.

How do Hackers Hack?

Photosani / Shutterstock.com

We hear about hackers hacking all the time. But how do they really do this? What is the actual "hack" of the matter?

There are plenty of ways a hacker can get what they want from a company, a person, or an agency, but here are a few of the most popular methods of attack.

Social Engineering

This category is especially stressful because social engineering is not thwarted by super tough software or a ridiculously prepared security firm. Social engineering exploits the individual people inside an organization; it's one of the cheapest and most effective ways a hacker can get what he or she wants. But what exactly is social engineering?

Social engineering is a special form of intrusion that can entail a variety of actions that use manipulative tactics to encourage people to drop standard security protocols. Anything from downloading a malicious link to conveying login credentials over the phone to holding your passcode-protected door open for the next person is considered social engineering. In these situations, hackers utilize social techniques to make you 'do' or 'say' something you normally wouldn't do or say.

For example, a man calls you on the phone and claims to be a technician from your internet provider. He says there's an issue with the network, and to make sure your business is unaffected by this problem, he needs your admin's login credentials. He assures you that everything will be super quick, and you'll avoid a lot of downtime. Appearing to be a no brainer, you quickly hand over your credentials not knowing this technician is really a hacker from across the country. Instead of avoiding downtime, you just created a lot of it… by handing over the keys to all your data.

Vulnerabilities

Software, browser, and system vulnerabilities are an easy in for hackers. Kaspersky Lab states that a vulnerability "is associated with some violation of a security policy." This violation allows cyber criminals to hide malicious code, unauthorized commands, or malware onto your computer.

The majority of vulnerabilities are eliminated when (or if) you update your workstation; however, many people fail to update their PC with the recommended updates when they become available (choosing to postpone or ignore a critical update). For example, about 30% of users are using an outdated browser, and nowadays, with vulnerability hacking like Malvertising, outdated browsers are creating an even bigger security concern.

With Malvertising, cyber thieves purchase ad space on a website and embed code in the ad. When you land on a website with a malicious ad, the imbedded code will search your computer for vulnerabilities and push malware into them. You don't have to click or view the ad to be infected; you simply have to visit the website. And the worse part about Malvertising is that it can be any website—rare or well-known. Google, Yahoo, Reuters, Forbes, The Daily Mail, and Huffington Post have all been previous victims of Malvertising—potentially infecting millions of people in less than a few hours.

The best defense against vulnerabilities is to make sure that all your technology is up-to-date at all times. Check your browser, operating system, software, and applications for updates on a regular basis and never postpone an update when one becomes available.

Rawpixel.com / Shutterstock.com

Be a more creative leader with these 3 tips

Part of being an entrepreneur and a business owner (and even to a certain extent a manager, supervisor, or team leader), deals directly with that creative spark inside you. FastCompany, a site dedicated to delivering entrepreneurs daily blog content, says it well, "First things first: There's really no such thing as an un-creative entrepreneurship." In other words, the simple fact that you've built a business points to a certain level of creativity.

However, this doesn't mean you have enough creativity to fuel the innovation or permanency of your business for years to come.

Everyone is capable of growing their creativity—of discovering new products, ideas, processes, relationships, projects, and so on, for many years. You simply have to be willing to embrace what it is to be creative.

Be willing.

Much of creativity deals with uncertainty and a large amount of vulnerability, and if you expect to be innovative and progressive, then you need to be okay with these two emotions. You need to be willing to be uncertain of an outcome—will you succeed or will you fail? And, you need to be willing to be vulnerable—what will the outcome be, your critics say, and your supporters demand?

Be inspiring.

You can try to run a business on your own but odds are, it won't be easy and you won't be successful. You need supporters; you need a team that is willing to stand for, by, and with your creativity. Inspire your team and those around you, and your ideas will be stronger and more prosperous. As an added benefit, your staff will be inspired to create and innovate, as well.

Be positive.

Since being creative means being vulnerable and uncertain, it's very easy to be swayed by negativity; however, the more negative you are, the more you'll fail to see the opportunity in circumstances (whether these circumstances are good or bad). Not only this, but how are people supposed to believe in your creations if you don't believe in them yourself? Think positively, and your creativity will grow to do bigger and better things.

Are you ready to update your router? Check out this touch-screen Wi-Fi connecter.

We've gone so far with our technology. Everything is connected to each other, and our gadgets are getting smarter every day. But if this is the case, why is our router—the very thing that allows us to connect our devices—so outdated? So basic, yet so confusing? So very uninspiring?

Well, TP-Link hopes to change this.

Introducing the AC1900 Touch Screen Wi-Fi Gigabit Router. This one-of-a-kind internet connecter replaces your mundane push-to-start router with a bright, crisp touchscreen display.

There's no longer a need to control your setup through a PC, smartphone, or extra device with AC1900. From one easy-to-use screen, you can control your connection settings, as well as who accesses your internet connection. For example, when you tap on the "Access Control" icon from the touchscreen, a list of all the devices connected to your network will display. Swipe any unwanted device off the screen to immediately and effortlessly eliminate access. It even comes equipped to handle parental control settings so you can easily manage your children's time spent on the internet.

With beamforming technology, AC1900 will attempt to rid your world of weak connections and dropped signals once and for all. Three separate antennas focus signals directly towards connected devices to provide stronger, more reliable connections for up to 10,000 square feet of coverage. And with a connection speed of 1900mbps, multiple devices can stream videos and play games at the same time—no lagging, no dropping, no pausing.

The AC1900 Touch Screen Wi-Fi Gigabit Router can be purchased on multiple sites like Staples, Jet, and Quill for an average price of $180.

www.tp-link.com