frogworks

Managing Your Technology So Your Business Doesn't Croak.

December 2021

Issue 12 Volume 11

Ribb"IT" Review

INSIDE THIS ISSUE:

Holiday Shopping Scams! The Worst!

How was your Thanksgiving? Great, we hope!

How about Black Friday? Cyber Monday? Are you in to those type of things? Personally, I typically avoid these shopping rushes in general, but there's no question they're incredibly popular and overwhelmingly successful.

So if you do participate – heck, even if you simply plan on shopping at all online this holiday season (like 100% of us do), you have to beware: **scammers want in on that holiday gift budget.**

RED FLAGS

- **Searching the Better Business Bureau** online directory, can tell you if the business your trying to buy from is accredited. In addition to checking the BBB listings, the Federal Trade Commission says to make certain the website includes a physical address and a phone number, and verify them. That way you have a place to contact should things go wrong.

- **Fake Shipping notices.** Legitimate carriers will never ask you for personal information through email. These are fake email delivery notices DO NOT click on any links.

- **Santa Phishing**. Several trusted companies offer charming and personalized letters from Santa, but scammers mimic them to get personal information from unsuspecting parents. Check with the BBB to find out which ones are legitimate.

- **Common charity scams** include look-alike sites or imposter websites, or phony emails that are "phishing" for personal information or giving a check or cash to an individual as opposed to an organization.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Common Insider Threat Profiles

Insider Threat Profiles come in many different shapes and forms and can be a frustrating problem to diagnose. Adding to the problem is the fact that even the most reliable and seemingly harmless employees can change in an instant and pose a threat. Protecting your company against these sometimes-unpredictable actors requires an understanding of the various profiles that exist and their motivations. To help, here is a quick look at some of the most common Insider Threats that companies may face, and some quick tips on how you can protect your organization from each of them.

Oblivious Oliver

Oblivious Oliver is the employee who has no clue that he is introducing risks to the organization. A large percentage of cyber security incidents start with human error. A prime example is a simple click on a phishing email leading to the compromise of approximately 40 million records.

The best solution for Oblivious Oliver's is training and awareness. By helping Oliver understand the risks of clicking on malicious links and encouraging him to approach all emails with caution, attempted phishing attacks against the Oblivious Oliver's of this world are less likely to succeed.

3rd Party Patrick

Third party contractors and vendors often have the same or very similar access privileges even though they aren't directly employed by the company. Their introduction of risks to the company can be intentionally or unintentionally malicious depending on the circumstance.

In most cases, the company realized significant losses as a result of their partner's actions, or lack thereof. This makes having a strong third-party security program that includes both technology controls and legal controls against a third-party breach imperative to stopping 3rd Party Patrick dead in his tracks.

Terminated Tony

Noticing activity from the account of someone who's been recently terminated? As Terminated Tony leaves, he creates back doors and tries to retain access to systems and data for future use. This is an unfortunate and costly mishap that occurs quite frequently. Ensuring that after an employee is terminated, access to systems throughout the company and network are promptly terminated is an important step to ensuring that Terminated Tony doesn't wreak havoc on your company after he's gone.

Malicious Marvin

Unfortunately, some insiders are just downright criminals. Employees steal from their employers for numerous reasons and are deliberately looking to breach the company's security and take advantage.

Malicious Marvin is a very real threat. Life happens, and unfortunately, even the best employees make poor choices. It's important to apply the concept of least privileged access and only grant access to users on a need-to-know basis. Furthermore, having insight into user activity through logging and monitoring, implementing a robust data loss prevention program, and having strong detection and response capabilities can help keep Malicious Marvin at arm's length within your organization.

Conclusion

Protecting your organization against an Insider Threat requires that you first understand what those potential threats might be by familiarizing yourself with Insider Threat Profiles. Oblivious Oliver, 3rd Party Patrick, Terminated Tina, and Malicious Marvin can cost your company millions of dollars if gone unchecked. This list provides insight into some of the most common insider threat profiles but remember that there are no limits to the motivations and profiles of Insider Threats. Anyone from business colleagues to your cyber security team could potentially pose a threat. This makes having a robust cyber security program based on the principle of "defense in depth" essential to stopping the insider threat.

The Importance of Building Company Culture

We have come to a day and age in which we are all trying to navigate a candidate-driven job market. This can be both a good and a bad thing. On one hand, you've got candidates being pickier about their next move, which means that retention rates are getting higher, and it seems to be a better fit for both sides. On the other hand, you've lost a lot of negotiating power, especially if you're working with a strong, well-rounded candidate that is wanted by multiple different companies. Dallas has the fifth-largest tech labor force in the US, behind Silicon Valley, D.C., and New York City. According to the same website, CBRE estimates that more than 160,000 DFW residents work in the technology field. With so much competition, it can be hard to hire and keep great talent. However, the best way to do that is to build a company culture worth believing in.

There are three steps to building and maintaining your company culture:

Implement

Once you've got an idea of what you want to accomplish, put it into place. Introduce things slowly, and make sure your current staff is on board. From there, bring in your newbies and help shift the culture to what you want it to be.

Lay It Out

In order to build a company culture, you've got to lay out what you want it to look like. Are you trying to build a "work hard, play hard" environment? Or a buttoned-up and professional environment? Maybe you want to make your office dog-friendly or cater lunch once a week for your employees. Whatever it is, you have to start somewhere. Write down your company's values, mission, and goals. From there, you can find and attract candidates that have similar views.

Study and Revise

It is imperative to continue to study the culture and revise as needed. If you see that something isn't working, change it! I will say that consistency is key, so when you find something that works, stick with it. Building traditions, allowing employee engagement are crucial to making it successful.

Building a company culture is extremely imperative to growing and maintaining a workforce. Now more than ever, candidates are looking for things that set companies apart – what will make your company a home rather than a stepping stone? Creating a culture and then hiring to fit within that culture makes retention much easier, as everyone has the same buy-in, beliefs, and values, and the expectations are set up front. Employees spend more time at work than they do with their own families, and they aren't afraid to ditch jobs that don't appreciate that. Appreciation goes a long way – as does a strong company culture.

Don't Fall For This Cryptocurrency Giveaway Scam

You know you've hit the Big Time when you get a scam named after you. That's exactly what has happened to Elon Musk. The latest scam that's making the rounds is called the "Elon Musk Mutual Aid Club" or the "Elon Musk Club" for short.

If you're an experienced IT professional it is easy to be dismissive of things like this. Few seasoned professionals ever fall for these scams after all.

The truth is that the scammers running these plays have made hundreds of thousands of dollars a day doing it. There are enough people on the web who are susceptible to the social engineering tricks they employ that the scammers can count on regular paydays.

Most scams of this variety have played out in something close to real time on a variety of social media channels. The drama of the Elon Musk Club however is playing out in email accounts around the world.

Although this scam invokes the name of Elon Musk and leverages his cult of personality to entice recipients the scam itself is pretty straightforward. It begins with a phishing email that includes a descriptive and enticing tag line. It reads something to the effect of "Get Free Bitcoin via the Elon Musk Club" or "Join the Elon Musk Club" or similar.

The scammers didn't waste any time trying to come up with a convincing message for the body of the email. It simply contains a link that points the way to a poisoned website. This page promises to give you 0.055 to all users who participate. The page contains an "Accept an Invitation" button which brings you to an information capture page. Just give your information away (including a photo of yourself) to sign up!

Except of course when you do you're just handing personal details to the hackers. What is worse is that before you can get your 0.055 you've got to donate 0.001 Bitcoin to another member of the club (supposedly chosen at random).

Naturally when you give the Bitcoin away you never get anything back and the scammers walk away with a tidy sum. Don't fall for it.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward

NEXTGEN

MSP TO WATCH • 2021 WINNER