Cybertools, Inc.
10410 187th St E
Puyallup, WA 98374

Inside This Issue

IS THAT A REAL TEXT FROM YOUR CEO? OR A SCAM?

Imagine you're going about your day when suddenly you receive a text from the CEO.

The head of the company is asking for your help. They're out doing customer visits and someone else dropped the ball in providing gift cards.

The CEO needs you to buy six $200 gift cards and text the information right away.

The CEO promises to reimburse you before the end of the day. Oh, and by the way, you won't be able to reach them by phone for the next two hours because they'll be in meetings. One last thing, this is a high priority. They need those gift cards urgently.

Would this kind of request make you pause and wonder? Or would you quickly pull out your credit card to do as the message asked?

A surprising number of employees fall for this gift card scam.

There are also many variations. Such as your boss being stuck without gas or some other dire situation that only you can help with.

Without proper training, 32.4% of employees are prone to fall for a phishing scam[1].

Variations of this scam are prevalent and can lead to significant financial losses, both personally and in the business.

In one example[2], a woman from Palos Hills, Illinois lost over $6,000 after getting an email request from who she thought was her company's CEO about purchasing gift cards for the staff.

Need Help with Employee Phishing Awareness Training?

Give us a call today to schedule a training session to shore up your team's defenses.

TIPS FOR AVOIDING COSTLY PHISHING SCAMS

1. ***Always Double Check Unusual Requests***

Despite what a message might say about being unreachable, check in person or by phone anyhow.

If you receive any unusual requests, especially relating to money, verify them.

Contact the sender through other means to make sure it's legitimate.

2. ***Don't React Emotionally***

Scammers often try to get victims to act before they have time to think.

Just a few minutes of sitting back and looking at a message objectively is often all that's needed to realize it's a scam.

Don't react emotionally, instead ask if this seems real or is it out of the ordinary.

3. ***Get a Second Opinion***

Ask a colleague, or better yet, your company's IT Service Provider, to take look at the message. Getting a second opinion keeps you from reacting right away. It can save you from making a very costly judgment error and only takes a few extra minutes.

Sources

1.https://itsupplychain.com/1- in-3-employees-fall-forphishing- attacks-withouttraining/

2.https://abc7chicago.com/scam-email-fake-boss-from/5901884/

Cybertools Chronicle

Insider Tips to Make your Business Run Faster, Easier and More Profitably

The 50th Law

By 50 Cent And Robert Greene

Fear is one of the greatest obstacles any entrepreneur or business leader will face. They fear they'll make a mistake that will cost their business thousands of dollars, or they might worry their product or service isn't good enough. These fears can become so intense they could even cause a business to fail.

Many entrepreneurs have tried to overcome their fear, and now *The 50th Law* by Robert Greene and 50 Cent is here to help. *The 50th Law* explores the concept of fearlessness and takes a deep dive into courageous entrepreneurs who held nothing back in order to achieve their goals. 50 Cent shares the business and personal plans that helped him escape poverty and the chronic fear he felt in his early years. This philosophical read is definitely worth checking out because it will encourage readers to put fear in the rearview mirror.

March 2023

This monthly publication is provided courtesy of David & Aubri Stone, Owners of Cybertools, Inc.

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

Keep Your Business Protected By Becoming Aware Of The Most Common Types Of Cyber-Attacks

The rate of cyber-attacks has significantly increased over the past few years. Businesses of all sizes are at risk of becoming victims of them, which is why it's crucial that every business owner and leader is aware of the most common cyberthreats impacting the business world today. Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals.

These criminals' tactics will improve as technology continues advancing, but cyber security defenses will as well. Knowing exactly what you're up against with cyber-attacks and creating the proper safeguards will protect your business. If you're new to the idea of cyber security or need an update on the common threats that could impact your business, we've got you covered. Below, you will find the most common types of cyber-attacks out there and how to protect your business from them.

Malware

Malware has been around since the dawn of the Internet and has remained a consistent problem. It is any intrusive software developed to steal data and damage or destroy computers and computer systems. Malware is an extensive type of cyber-attack, and many subcategories belong to it, including viruses,

Continued on Page 2 ...

... Continued from Cover

> **"Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals."**

spyware, adware and Trojan viruses. One type of malware that has lately been used more frequently is ransomware. Ransomware threatens to publish sensitive information or blocks access to necessary data unless a sum of money is paid to the cybercriminal who developed it.

Unfortunately, malware can be detrimental to nearly every operation of your business, so you should do two essential things to prevent it from affecting your company. First, you should install the latest anti-malware programs. If you hire a services provider, they will take care of this for you. If not, you'll need to find anti-malware that works best for your system. You should also train your team about these risks and ensure they are aware not to click on any suspicious links, websites or files that could be dangerous.

Phishing

Have you ever received an e-mail asking for sensitive information that looked official, but something just wasn't quite right? Chances are it was probably a phishing scam. Phishing occurs when cybercriminals send official-looking messages to individuals, posing as another organization, in an attempt to receive personal information. Falling for a phishing scam can quickly result in you becoming a victim of identity fraud. The results can be substantially worse if a business falls for the scam.

So, how do you best prepare for and protect your team against phishing scams? Utilize employee cyber security trainings so they can spot the warning signs. The actual e-mail will usually line up differently from whom the cybercriminal is trying to represent. Also, most organizations will not request private information over e-mail. Common sense will prevail over phishing scams.

Distributed Denial Of Service

DDoS attacks can bring your business to a standstill. These attacks occur when malicious parties overload servers with user traffic, causing them to lag or shut down since they are unable to handle incoming requests. If your business falls victim to this kind of attack, your employees might not be able to access key functions required to do their jobs, and customers may not be able to use your website or purchase items from you.

DDoS attacks are very difficult to thwart, and a determined cybercriminal can lock up your websites and networks for days on end. You'll have to identify malicious traffic and prevent access before it can cause damage. Hiring an MSP is your best bet to prevent DDoS attacks. If a DDoS attack is successful, you'll probably have to take your servers offline to fix the issue.

Password Attacks

If a cybercriminal gets your password or another employee's password, this is the easiest way for them to access your valuable information. They may attempt to guess the passwords themselves or use a phishing scam to gain access. It is vital that you enable multifactor authentication for your employees and require complex passwords so you can defend your company against password attacks.

Now that you know the most common forms of cyber-attacks currently happening, you can take the necessary precautions to protect your business, employees and customers.

Free Report Download: NEW And Critical Changes To Cyber Security, Insurance Coverage And Threats That Will Put Your Business At Serious Risk If Not Addressed Immediately

Discover what the vast majority of businesses don't know and haven't been told about changes to cyber security risks, insurance requirements and threats that are allowing them to operate at UNDERAPPRECIATED RISK for a crippling cyberattack and subsequent costs, lawsuits and fines – and what to do about it now. Don't think you're in danger because you're a "small" business and don't have anything a hacker would want? That you have "good" people who know better than to click on a bad e-mail or make a mistake? That it won't happen to you? That's EXACTLY what cybercriminals are counting on you to believe. **It makes you easy prey because you put ZERO protections in place, or simply inadequate ones.**

Get your FREE copy today: www.cybertools.us/3-surefire-signs

Cartoon Of The Month

"I realized I have too many high-tech gadgets when I became Facebook friends with my toaster."

SHINY NEW GADGET OF THE MONTH

Valve's Steam Deck

Nintendo, Microsoft and Sony are some of the most prominent players in the video game console industry, but there's another name making headlines in these console wars: Valve's Steam Deck. In fact, this is the perfect gaming system for anyone who is looking for a powerful and portable console.

The handheld system is capable of playing the most advanced AAA games available and comes in three different storage sizes. If you've used Steam in the past on your PC, you'll immediately gain access to your library of games and will be able to purchase any other games from Steam directly on the device. Check out the Steam Deck if you're in the market for an affordable, powerful and portable gaming PC.

HAVE YOU HAD DATA EXPOSED IN A RECENT DATA BREACH

There's a reason that browsers like Edge have added breached password notifications. Data breaches are an unfortunate part of life. And can have costly consequences for individuals. Hackers can steal identities and compromise bank accounts, just to name a couple.

Cybercriminals breach about 4,800 websites every month with form jacking code. It has become all too common to hear of a large hotel chain or social media company exposing customer data.

- Microsoft Customer Data Breach
- 5 Million Records Exposed in a Student Loan Breach
- U-Haul Data Breach of 2.2 Million Individuals' Data
- Neopets Breach May Have Compromised 69 Million Accounts
- One Employee Computer Causes a Marriott Breach
- Shield Health Care Group Exposes Up to 2 Million Records

The Most Important Word In Business?
It's Not What You Think

A video podcaster recently asked me, "What's the most important mindset for success in business?" For a moment, I doubted I could identify just one key mindset for success. As trusted advisors to CEOs and investors of large companies, our consultants at ghSMART typically emphasize the importance of context.

For example, there is no "perfect candidate" to hire for a job. Success depends mostly on a leader fitting a given context, which has many variables – the customer landscape, strategic challenges, operating challenges, financial or legal factors and culture (among other things).

But then it dawned on me. There is one mindset that I have observed in successful versus unsuccessful ventures. The most important word in business, which you rarely hear, is *generosity*.

Leaders who succeed are generous and treat everyone with a fundamental mindset of generosity. In contrast, people who lack a spirit of generosity fail in the long run. Over the years, I've witnessed many examples of both selfishness and generosity. Here are a few lessons you can learn from my own experiences.

(Don't) Trick The Customer: Once, while talking with the CEO of a mortgage company, I instantly got a bad feeling about his character. His mindset was selfish. He implied that his business succeeded by "tricking" low-income homeowners into signing up for mortgages with hidden terms that were unfavorable to them. Well, that mindset backfired. When the housing crisis happened in 2008 and 2009 (caused partly by bad actors like this guy), a pile of lawsuits snuffed out his company and career.

(Do) Create Unexpected Experiences: At ghSMART, one of our colleagues, Alan Foster, expressed an interest in improving his "storytelling" skills. Alan is a charming Brit who leads our UK office. For anybody who knows him, they understand that he's already a fantastic storyteller, but he just wanted to take his game up a notch – to dazzle audiences when he gave talks about leading talented teams. Some other colleagues took the initiative to research opportunities and found an upcoming two-day seminar hosted by a star Hollywood movie screenwriter and master storyteller. They got Alan admission to this exclusive seminar, comped the cost and gave the experience to him as a present. How cool is that? Can you imagine working at a firm where people look for ways to give you what you need or want? As the chairman and founder, I am very happy to see our culture of generosity and gratitude continue to blossom as we grow.

Wall Street's Gordon Gekko may have said, "Greed is good," but a mindset of generosity is better, especially if you want to succeed in your career and live a fulfilling life.

We are so grateful for the relationships we have been entrusted with throughout the years. We believe that the greatest form of flattery is a referral we receive from friends and satisfied clients. A great referral for us is a business with 25-500 users. Go to **www.cybertools.us/about-us/referral-program**