NEWSLETTER

■ February 2020

TRAIN YOUR STAFF BEFORE YOUR BUSINESS BECOMES AT RISK!

Reduce staff-related incidents, protect office confidentiality, and avoid office disasters by implementing a training program with our suggestions.

Clean Desk Policy

Sensitive information on your desk in the forms of sticky notes, documents, and printed materials can quickly be taken by passersby. Make it a point to have your employees have a clear desk policy. When not at their desk, remind them to place these documents in a locked drawer.

BYOD Policy

Bring-your-own-device allows employees to bring in their own devices, but remember to have a list of acceptable and banned devices, allowed applications specified in writing, and remind your employees that they will be monitored continuously, and should have the latest antivirus program installed at all times.

Data Management

Having a backup copy of customer contracts is good business practice. Employees should be aware of all the types of data, so they can understand everything that goes into contributing to a prosperous business.

Removable Media

Unauthorized removable media is a risk for your business because it may impact data security issues, malware infection, hardware failure, and copyright infringement. Emphasize the importance of not allowing stray media (such as external hard drives) to enter your business proximity.

Safe Internet Habits

Provide training on safe internet habits to counteract cybercriminals from impacting your organization.

- Disable pop-up windows
- Do not open attachments

Continued on page 2

COMPUTER MAGIC

Welcome to our monthly publication provided to you by Samantha Boneck, Marketing Associate of Computer Magic, Inc.

Our Mission: We help you reach your long-term objectives, enable you to drive real growth in your company, and to secure greater return on investment.

WHAT'S NEW

All of us at Computer Magic would like to wish everyone a **Happy Valentine's Day** filled with love, compassion, and kindness. Please be aware that we are in the process of building a new website and social media platforms.

With Valentine's Day just around the corner, we at Computer Magic would like to offer chocolates to a lucky winner. This lucky person could be you: all you must do is to **be caller number 14!**

We look forward to hearing from you!

Samantha Boneck
Marketing Associate
Computer Magic, Inc.

Continued from page 1

from unknown sources or suspicious links

- Educate employees on the warning signs of phishing attacks
- Do not install software from unknown sources

Social Networking Dangers

Teach how phishing attacks target social media platforms and what your employees need to do to keep information protected. Additionally, point out the importance of maintaining a close eye on well-known sites with slight differences such as www.yahooo.com.

Email Scams

Include tips to make employees aware of email scams and what they need to do to avoid this from happening to your employees.

Top tips to keep in mind:

- Do not trust unsolicited emails
- Do not send funds requested by email
- Always filter spam
- Keep antivirus and firewall programs up to date
- Do not click on unknown links in email messages
- Be extra careful of email attachments

> “
> ***True happiness is to enjoy the present, without anxious dependence upon the future, not to amuse ourselves with either hopes or fears but to rest satisfied with what we have, which is sufficient, for he that is so wants nothing.”***
>
> ***Seneca***

PROTECT YOURSELF FROM THESE COMMON ATTACKS

Everyone can benefit from learning how to keep their information secure. Getting in the habit of protecting websites and online services is key to not becoming a victim of cyberattacks. And knowing website security will aid in getting a better understanding of cybercriminal attacks.

Be aware of these trends:

1. Web Application Firewalls (WAFs) are hardware and software applications that you can use to block threats. Think of it as a gatekeeper for all incoming traffic, blocking malicious threats that would otherwise gain access and infect your system. WAF applications can protect your website against SQL injection attacks.

2. Cross-site scripting (XSS) occurs when lines of malicious JavaScript code are injected into a webpage to target the website’s users.

These scripts target user sessions within a website’s search bar or comments where the user redirects to a malicious website.

3. Malware ranges from viruses to adware that has the potential to affect both computers and websites. Malware scanning, removal, and prevention, if implemented, prevents this from happening.

4. Interception is just as it sounds; the hacker intercepts data that users submit to a website and use it against the user. It’s best practice to secure your website with an SSL certificate to protect sensitive information.

5. Keylogging is the process of recording every keystroke made by the user, which then returns to the hacker. Always use strong passwords and initiate 2-step authentication.

6. When a website is receiving vast amounts of traffic or requests that overwhelm the system, you may become at risk for **Distributed Denial of Services attacks (DDoS)**.

Botnets generate fake-traffic from computers that attack, and as a result, the website loads poorly. The protection of advanced security monitoring and WAF can prevent this type of attack from occurring.

7. Security misconfiguration occurs when the security settings on a website have holes or weaknesses that lead to vulnerabilities. Proper website maintenance or correct web application configuration is needed.

Leaving your settings as the default makes it ridiculously easy for hackers to gain access to the backend of your website.

Awareness of the types of attacks that exist is the first step towards protecting your company from cybercriminals.

Godaddy.com, Oct. 5, 2018

CYBERCRIMINALS DON'T WANT YOU TO KNOW THESE SECURITY MEASURES

According to Statcounter, users in the US use their smartphones 54% of the time compared to computers, currently at 41.3% and tablets at 4.69%. In today's world, we use our smartphones more than we use computers or tablets, but how often do we take measures to protect our devices?

Security for your smartphone:

- **Install security software on your device**
- **Create stronger passwords**
- **Keep software up to date**
- **Check bank statements and mobile charges frequently**

Practicing these techniques will create a barrier against cybercriminals stealing your private information and could be the difference between keeping your good credit score or ending up with nothing. Please practice common sense before you click!

THE SECRET TO CYBERSECURITY

by Scott E. Augenbaum

Cyberattacks have become frequent to the point that everyone needs to be aware of how cyberattacks work so they can have a basic understanding of how to avoid them. Let's go back to 2014 when Home Depot was compromised or when hackers infected payment card readers at Target in November of 2013.

Dr. Michael McGuire, a senior lecturer at the University of Surrey in England, found that cybercrime revenue around the world has grown to 1.5 trillion in illicit profits per year, which is roughly equal to the GDP of Russia. And it is planned to rise to 6 trillion by 2021.

In his book, Augenbaum writes on essential topics such as phishing attacks, mobile device safety, password safety, 2-factor authentication, social media safety, among other safety topics that you may not be practicing right now. The three most relevant issues I would like to focus on are strong passwords, 2-factor authentication, and social media to provide you with an in-depth review of the importance of taking precautions to protect yourself.

Creating Strong Passwords

The average person has a straightforward password, which is extremely dangerous, but very convenient for the user to remember.

For example, a strong password should include 15 to 24 characters, upper/lowercase letters, numbers, at least one special character, and must not have any words found in the dictionary. Practice two methods to have a safe password!

(1) Decide your favorite number and a special character, and DON'T write it down or share it with anyone! Memorize them!

(2) Think of a simple passphrase that's easy to remember. For example, "I love to shop at amazon very much." Keep it simple!

Take every first letter in the sentence of your passphrase, replace 'I' with the number 1 and insert @ for one of the 'a's, and replace the word 'to' with the number 2 while incorporating your chosen numbers and special character. In this example, I'm going to

Continued on page 4

IT Security Tip of The Month

PHISHING

The Federal Trade Commission's OnGuardOnline provides with examples of what cybercriminals ask when attempting to steal your information. Please review the following:

- *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*
- *"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."*
- *"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."*

Tips to keep in mind

1.) Have a doubt? Throw it out! Links within emails and online posts are the best way in for cyberthieves. Always trust your gut! If you have any suspicion, even a little bit, contact the company directly (via phone) to check if the email came from the company.

2.) Think before you click! If it sounds too good to be true, it probably is! If you receive an email requesting immediate action, don't do it! Never give out your personal information without doing research.

3.) Use stronger authentication. Authentication tools assist in the verification of a user. It's always good to double-check!

4.) Make your passwords complicated. Use capital and lowercase letters combined with symbols and numbers.

5.) Install and update anti-virus software. Regularly check for updates on Anti-Virus software, firewalls, email filters, and anti-spyware.

6.) Hyperlinks. Don't rush to click on hyperlinks in an email! Instead, type the URL directly into the address bar. Check hyperlinks by hovering the cursor over it to reveal the full address. *Dhs.gov*

Continued from page 3

choose 4 and # at the beginning of my password, then reversing it at the end to create 4#1l2s@avm#4 (I love to shop at amazon very much) for my password, make sense? Reminder: **DO NOT** write down your passwords but instead write down your passphrase, "I love to shop at amazon very much" and keep it in a safe place such as on a piece of paper in a book. You will have to memorize your chosen number and special character. Don't write them down! Your number and special character will stay the same for all your passwords; it's the passphrase that will change each time. Eventually, it would be best if you were memorizing your passphrase, but this may take time, which is why we are asking you to keep them safe in the back of a book. Memorizing the passphrase may come off as impossible for some of you to do but, could mean the difference between losing all your hard-earned money or keeping it stored within your mind and having the peace of knowing your accounts are safe.

Malicious attacks are far too frequent today. Cybercriminals are targeting you because of our simplicity with passwords and the lack of knowledge when it comes to cybersecurity.

2FA Authentication

The reasoning behind why 2FA (two-factor authentication) is so essential is that it gives you that extra layer of security, making it more difficult for criminals to snag your personal information. Follow these precautions:

- Use emails that offer 2FA such as Google, Outlook, and iCloud,
- Download an authenticator app like Google Authenticator
- Do not access your email accounts from untrusted devices. Only access email from computers and mobile devices that you own

Using strong passwords and 2FA is a great way to provide an extra layer of protection for your information.

Social Media Safety

Social media has become very popular among the cybercriminal community. If these attackers get your Facebook login and password, they could go on to write a post in your name and insert technology within that post to steal your information. Practice these techniques to stay safe:

- Install two-factor authentication on your social media platforms,
- Don't click on links sent via social media through emails or messages,
- Don't share personal information (social security number, birth date, home address, phone number, or work history) on social media.
- Continue to use 2FA, as discussed above, and for your social media accounts.

TECH TRIVIA QUIZ

ENTER TO WIN!

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a **$25 Amazon gift card**. Ready? Call us with your answer!

Before being known as PayPal, the company went by what name?

A) Confinity
B) MoneyMate
C) The X-Change
D) iCash.com

Call us right now with your answer!

608-291-9723

Children of baby boomers: make sure your parents don't become targets

Adults 60+ are targets for cybercriminals to attack. Individuals born between 1946 to 1964, may not know who to contact, they're too ashamed to make a report, or the worst of all, they aren't aware that they have become a victim.

Don't give control to the cybercriminals: use these techniques:

1.) Do not give remote control of your computer over to a salesman or technician,

2.) Be wary of anyone with an "urgent" message to complete a task,

3.) Do not trust caller ID,

4.) Keep software, firewalls, and pop-up blockers up to date,

5.) Do not trust phone numbers advertised in a pop-up on your computer screen,

6.) Only call well-known companies for computer repairs or, go in-person,

7.) If you receive a call from someone offering you a refund on an antivirus software subscription, hang up immediately!