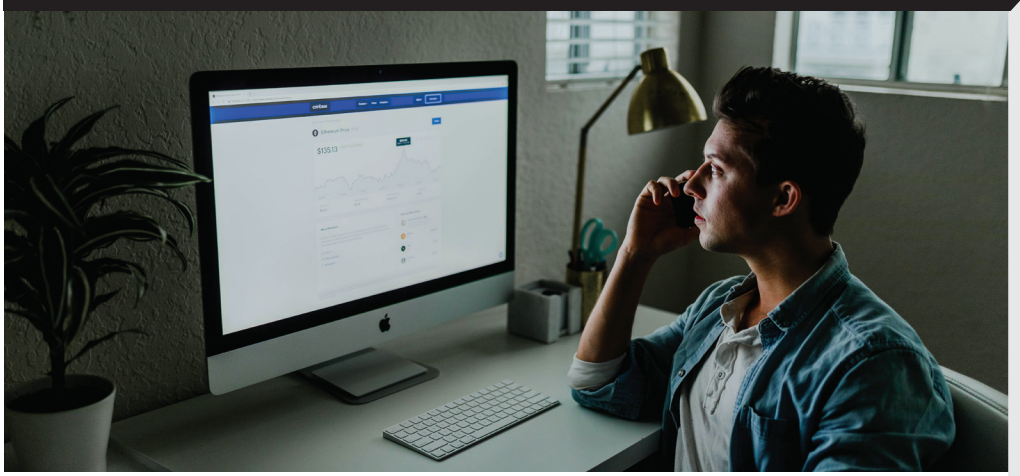
NEWSLETTER

■ April 2020



DON'T ALLOW YOUR EMPLOYEES TO BECOME TARGETS

Small businesses are the biggest targets of hackers and cybercriminals. Why? Because small businesses are less likely to have security in place. But in so many cases, hackers don't need to use malicious code or cracking skills to get what they want. Instead, they rely on your most significant vulnerability: your employees.

The #1 threat to any business's IT security is its employees.

It all stems from a lack of training. Employees don't know how to spot threats, or they don't know to click unverified links in their e-mails. Most of the time, these actions are simple mistakes – but mistakes aren't excuses and can result in MAJOR costs to your business.

Here are three things you can do to turn your employees from your biggest IT threat to your biggest IT asset:

Establish Regular Cyber Security Training.

First and foremost, get everyone in your business trained up on IT security. Wesley Simpson, the chief operating officer of (ISC)2, an international cybersecurity certification group, suggests thinking about IT education as "people patching." Just as you continually update and patch your software and security, ongoing training serves to update, or patch, your employees. He says, "If you don't get your people patched continually, you're always going to have vulnerabilities."

But don't put the training solely on your shoulders. Work closely with a company that specializes in IT security. Doing it yourself can be stressful and time-consuming. An experienced IT firm is going to come in with all the education and resources you need to successfully train everyone in your organization on cyberthreats targeting your business today.

Keep Cyber Security Top of Mind.

While you may have training or educational sessions once a quarter or biannually (we recommend regular sessions), you still need to keep IT security in the minds of your employees weekly.

During weekly meetings, for example, talk about a cybersecurity topic. Or, if you share news or links with your employees in a weekly, company-wide email,

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

As of March 16, our staff is now working remotely. We will continue to follow the news as the COVID-19 continues to develop, and we will keep you informed as changed occur. Thank you for your patience and understanding during this difficult time. Stay safe!

Samantha Boneck
Marketing Associate
Computer Magic, Inc.

Continued on page 2

for example, include a cybersecurity story or tips article. It's all about utilizing systems you already have in place to keep your team informed, and this critical topic at the forefront.

Emphasize Safe Internet Usage Habits.

This should supplement regular training. Employees should always know the best practices when it comes to using the Internet, email or anything else that brings them in contact with the World Wide Web. Part of it involves keeping the lines of communication open. If an employee sees something out of the ordinary come into their inbox, encourage them to bring it to the team's attention – whether they're telling their direct supervisor, manager, or you. The smoother the communication between everyone on your team, the easier it is to identify and stop attacks.

The goal is to eliminate guesswork. If an employee isn't sure about an e-mail, train employees to ask questions and verify.

On top of that, you should have a policy in place that prevents employees from installing unverified software, which includes apps and app extensions (such as browser extensions), without permission. And one more thing – stress safe Internet usage habits not just in the workplace but at home as well. Safe Internet usage habits are especially critical if your employees are bringing in their own devices. If that's the case, you should have a "bring your own device" (BYOD) security policy in place. It's just another wall between your business and potential threats.

How do you get all this started? Good question! It all starts with reaching out. If you're ready to lock down your business and you're serious about educating your employees and turning them into your best defense, we can help. The best IT security you've ever had is one phone call away.

> ***"You've got to get up every morning with determination if you're going to go to bed with satisfaction."*** *George Lorimer*

MAXIMIZE PRODUCTIVITY BY SHIFTING TO REMOTE WORK

We now live within a time when practicing social distancing and self-isolation is mandatory (even if temporary). As we shift to working remotely, the future is inevitably going to change in the direction of having more remote workers.

To create an effective work-from-home environment for your employees by keeping these three considerations in mind:

Don't allow employees to use their personal computers or devices.

These devices could contain malware, viruses, and become easy victims of cyberattacks. Not everyone takes care of their personal computers the way they should or may not know how to install the proper protection or consistently do updates. Provide your employees with company-approved and secured laptops and devices for them to use as they work from home.

Secure employees WIFI access point

Don't allow cybercriminals to steal your employee's data with easy access points. WIFI is often broadcast far beyond the home and into open areas.

- Use strong encryption and a more complex password
- Hide your network name
- Use a Firewall

Use a two-factor authentication VPN

VPN is a private, encrypted tunnel that goes directly to your IT network within the office. By using 2FA, you're creating a double layer of protection because your employees will need to call into the office to access the network. Alternatives to VPN are 'Zoho' and 'GoToMyPC.' Using these in place of VPN may not be as secure, but it's better than having nothing.

IT Security Tip of The Month

COVID-19 CYBER ALERT

As we go into April, the COVID-19 epidemic has brought the attention of cybercriminals across the globe. You may think that during a world event such as this one, nobody in their right mind would even attempt to take advantage of a situation that involves so many people. It would be best if you kept in mind that during times like these, cybercriminals are on holiday, a cybercriminals version of Christmas. Fear and stress are two emotions that create excellent scam victims. When we're fearful or stressed, we don't think as clearly and are more susceptible to becoming victims of scams. With this in mind, we want you to be prepared for charity and phishing scams, practice caution with email attachments, and finding information from legitimate sources.

CYBER SAFETY TIPS

- AVOID clicking on links in unsolicited emails and always be cautious of attachments in emails. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Always use trusted sources – such as a government website – for up-to-date, legitimate information.
- Never reveal personal or financial information in an email and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Please review Charity Scams for more information.
- Review Risk Management for COVID-19

US Department of Homeland Security. Retrieved from cisa.gov/coronavirus

SECURITY TIPS FOR BUSINESSES TO PREVENT CRIME

During times of high crisis, your business may become a target to criminals who are willing to risk their health to make an extra buck. Never underestimate desperation!

If your business has been temporarily closed, follow these tips to stay safe:

- Review your security plans
- Remove ALL cash; leave cash drawers open and empty.
- Remove or secure important, valuable items
- Make sure your security system is operational and accessible.
- Check to make your security cameras are working and aimed in the right direction.

For businesses with reduced hours, follow these safety measures:

- Review security and staffing plans
- Control access to the business; maintain a safe spacing of at least six feet between people.
- Lock all doors not being used for operation during business hours.
- Train your staff to be observant and to report suspicious behavior.
- For deliveries, review safety plans with drivers, so they are on the same page as you.
- Check to make sure security cameras are working and point in the proper direction.

Fox 9. (24 March 2020). fox9.com/news/security-tips-for-businesses-to-prevent-looting-robberies-during-coronavirus-closures

EVENTS FROM HISTORY: APRIL 1

1948

The Origin of Chemical Elements

A paper published in the Scientific Journal Physical Review highlights the idea of the universe being created by the "big bang".

1976

A computer in a wooden box with 4K of memory

The Apple I Personal Computer could be yours for only $666.66. What a steal!

1983

Man decides to go for a walk...around the world

Steven Newman a.k.a "The World Walker" from Bethel, Ohio makes the decision to walk on the wild side. Over a period of 4 years, he experiences muggings, getting pelted with stones, arrested multiple times, and attacked by boar and bison. I can't help but to picture the scene from Forest Gump when visualizing Steven's journey.

2001

The Netherland's becomes the first country to legalize same-sex marriage

2004

Google offers e-mail with a gigabyte of storage

Free e-mail with 1 gig was unheard of at the time.

2008

Cheap Trick Day "Trickford" in Rockford, Illinois

Thank you, State Senator Dave Syverson!

2009

20th Anniversary of the Simpsons

USPS celebrates the popular tv show with a 1-billion stamp run. Only 1/3 are sold resulting in a $1.2 million loss, Ouch!

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!

The size of the computer's memory is measured by the number of:

A) Memory Space
B) Bytes
C) RAM
D) ROM

Call us right now with your answer!

608-291-9723

COMPUTER MAGIC

608-291-9723 computermagic.us
101 Nichols Rd, Monona, WI 53716
tom@computermagic.us