NEWSLETTER

■ July 2020

AVOID BEING HACKED BY PRACTICING THESE 3 CYBER SECURITY PROTECTIONS

Five years ago, you might have had state-of-the-art security protecting your business and network. You had the latest malware protection, highly rated firewalls, and a great data backup plan. Maybe you even had a handbook on how to address cyberthreats. You achieved your goals! But then you forgot to do one crucial thing: you didn't stay up to date with your IT security policy.

Not staying innovative is a trap countless small business fall within. They invest in top cybersecurity once. Five years ago, this was fantastic. The problem is that cyber threats are continually evolving. Methods used by hackers and cybercriminals have come a long way in the past five years. Criminals stay on top of what's going on in the IT security industry. They are always looking for new ways to steal your data and make a quick buck at your expense.

What can you do to stay up to date in an ever-changing digital world? Here are three things every business must do to protect itself.

Understand the Threats

It's easy to assume that hackers are trying to get into your network the "old -fashioned" way. You might picture them hacking your network, trying to get your passwords and usernames, or breaking through your firewall protection.

While some hackers will do this (it's easy for them to gain access if you use simple passwords), many of today's cybercriminals rely on social engineering.

The most common form of social engineering is the phishing scam. The criminal sends you or your employees an e-mail, hoping someone will click a link or open an attached file. Cybercriminals have gotten VERY sophisticated. These e-mails can mimic the look of a legitimate e-mail from a legitimate business, such as the local bank you work with or another company you buy from (or that buys from you). Social engineering is all about tricking people.

A cybersecurity handbook will allow you added protection –

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

Computer Magic is here for you! We're available 24/7 for anything you need. Reach out to us if you have any questions. And, remember to check us out on Facebook and LinkedIn.

To our valued clients, we now have a referral program with a $100 and $500 incentive.

Samantha Boneck
Marketing Associate
Computer Magic, Inc.

Continued on page 2

one that is regularly updated. It's something you can reference. Your team needs to know how to identify a phishing e-mail, and you need to have procedures in place for what to do if a questionable e-mail shows up. A cybersecurity handbook helps keep your employees from becoming the weak link in your security setup.

Continually Update

From software to hardware, you must stay updated. There is no such thing as "one-and-done" when it comes to network security. Something as simple as a wireless router can DESTROY your security if it's not regularly updated.

Hackers are always looking for vulnerabilities in both hardware and software, and when they find them, they WILL exploit them.

What happens when the manufacturer no longer supports your hardware (like a router)? Occurrences such as this happen all the time, particularly as hardware ages. Manufacturers and developers drop support for their older technology so they can focus on their newer products. When they drop support for a product you use, this is a good indicator that you need to replace that piece of hardware. The same applies to software.

You might balk at the cost of buying new technology, but the price is well worth it in the long run. Think of the cost of purchasing a new router versus cleaning up after a data breach. Some small businesses never recover after a hack – it's just too expensive. Keep your malware software updated, keep your firewall updated, keep your cloud backups updated, and keep all your devices and software UPDATED!

Invest in Proactive Network Monitoring

When it comes to the security of your network and overall business, being proactive can make a huge difference.

Active monitoring means your network will be protected 24/7.

Every little ping or access to your network is watched and assessed. When the IT specialist finds a threat, then it can be stopped before it causes damage.

The great thing about proactive network monitoring is that you can customize it. Want to know about every threat? You can request a real-time report. Only want updates once a day or once a week? That alternative is available too! This approach means you have one less thing to worry about and can focus on more critical aspects of your small business. Someone is always keeping an eye on your network, making sure the bad guys stay out.

You might think, "How am I going to do all this?" You don't have to go it alone – and you shouldn't. Work with an IT services firm. Work together to find the best solutions for your business. When you work with IT specialists, you can rest assured your team will have updates on today's threats. You'll know your network – and everything connected to it – is updated. And you'll know someone is watching over you. That's the ultimate peace of mind.

3 Critical Cybersecurity Protections EVERY Business Must Have in Place NOW to Avoid Being Hacked. (2020, June) techadvisory.org/2020/06/3-critical-cyber-security-protections-every-business-must-have-in-place-now-to-avoid-being-hacked/

PASSWORD SECURITY DO'S & DON'TS

- Use different passwords on different accounts
- Use the longest password or passphrase available by each password system
- Develop mnemonics to help you remember complex passwords
- Consider using a password manager such as LastPass.
- DO NOT use passwords based on personal information such as a child's name, pet, or high school.
- NEVER use a password found in a dictionary.

Security Basics

1. Keep your operating software and browser up to date.
2. Apply antivirus software and firewall protection.
3. Regularly scan your computer for spyware.
4. Always use caution with email attachments and links.
5. Continuously watch for suspicious activity on your accounts.

(2019, November 18). Choosing and protecting passwords. Cybersecurity & Infrastructure Security Agency. us-cert.gov/ncas/tips/ST04-002

REFERRAL PROGRAM

Refer a company with ten or more computers and at least one server to our office. Once we've completed our initial appointment with your referral, we'll give you $100. If the company then becomes a Client with Computer Magic, we'll send you another $500! **Call us for more information: 608-291-9723.**

IT Security Tip of The Month

DENIAL OF SERVICE ATTACKS ARE ON THE RISE!

The process involves a machine or network resource unavailable to its intended users by a cybercriminal who disrupts the services of a host connected to the internet. According to Kaspersky Lab, DDoS attacks have climbed to 84%, and the most dangerous day for an attack is typically on a Saturday.

These attacks range from Volumetric attacks (which are the most common) to Application-Layer attacks to Protocol attacks.

Tips to Prevent a DDoS Attack

1.) Secure your network infrastructure

Most standard network equipment comes with limited DDoS mitigation options. Outsourcing is beneficial for added layers of protection.

2.) Strong Network Architecture

Create redundant network resources

3.) Leverage the Cloud

The cloud has more bandwidth & support, it can absorb harmful & malicious traffic, and experts who deal with these issues daily manage the cloud.

4.) Be aware of the warning signs

When you experience slowness, spotty connectivity on the intranet, or intermittent website shutdowns, be on alert!

8 MONEY SAVING SECRETS FOR SMALL BUSINESSES

1. Focus on the small things

Regular waste can cost you from 1%-3% annually. This percentage may seem like a small number to a small business owner; however, with other costs such as office expenses, these little costs can add up.

2. Negotiate with your vendors

When one small business is affected, you can guarantee another small business is as well. Vendors want to keep your business during stressful times, and some are willing to negotiate a decrease in prices rather than lose you as a client.

3. Maintain 10% of annual revenue in cash

Having 10% of your annualized revenue in the bank will allow you to make the right decisions instead of acting out of desperation.

4. Amend recent tax filings

Review and amend the last three years of taxes to generate extra savings for your small business. Additionally, you can have your accountant look for potential missed deductions that could result in a very high return.

5. Be conscious of your spending

Look over your top expenses and calculate a return on investment for each. You can count "soft" or non-direct monetary returns.

6. Save a minimum of 5% per month

Saving 5% of your monthly revenue will allow you the freedom to have peace of mind in case something unexpected happens.

7. Improve your accounts payable/accounts receivable cycles

Extending your payables and speeding up your invoicing will save you cash. Another option you have is to barter - your vendors may be in a similar position and may welcome the ability to make a transaction without cash.

8. Adjust your advertising strategy

Have you considered the power of social media posts, word-of-mouth, blog articles, or email marketing blasts?

(2020, June 22). 14 Lesser-Known Money-Saving Tips for Small Businesses. Forbes. forbes.com/sites/forbesfinancecouncil/2020/06/22/14-lesser-known-money-saving-tips-for-small-businesses/#31fdc28e6768

> ***Life is made up of a series of tests, trials, and great opportunities. Some are momentary, but most take endurance."*** *Michael K. Simpson*

EFFECTIVE THOUGHT LEADERSHIP CONTENT

The benefits of providing effective content are significant! Small business leaders should adapt to the changes and try new things and embrace new ideas! Build your reputation, trust, drive sales, and improve profitability with compelling thought leadership content.

3 Characteristics of Effective B2B Thought Leaders

1. Add Deep Thinking and Intellectual Rigor to your Content

- Subject matter with emerging interests,
- High-quality research with objectivity,
- Include new topics to entice your audience,
- Allow for concrete actions your readers can apply.

2.) Implement a Strong Support System

- Effective communication between leadership and the sales team,
- Ensure coordinated production across your organization.

3.) Invest your time into Distribution

- Involve new trends and popular topics to breathe new life into your content,
- Reuse your content by making updates and adjustments. Make sure to add value!

How you can Impact Trust for your Brand

1. Subscribers are more likely to become customers

- A customer who trusts your content is going to trust your brand and embrace what you represent.
- Turn your traffic into subscribers and subscribers into customers.

2.) Powerful content will spread

- Your audience is more likely to read your content if they know you and respect your company.
- If an influential blogger discovers your content, it may go viral instantly.

3.) Allow your content to be easily absorbed

- Make your content memorable and invoke an emotional reaction.
- Your content should communicate an idea effectively and quickly understood by your audience.

AVOID these top attributes of low-quality content

- Don't repeat what you've already mentioned,
- Don't use basic or elementary concepts,
- Don't turn your content into a direct sales pitch. As a rule, people don't respond well to being sold; instead, inform them of their options.

Let's look over the compelling statistics of effective content:

- 48% of decision-makers spend an hour or more reading through thought-provoking content,
- 89% of decision-makers say compelling content can enhance their perceptions of an organization,
- 49% of decision-makers say that thought leadership can be useful in influencing their purchase decisions.

Strong, F. (2020, April 4). The 3 Characteristics of Effective Thought Leadership in B2B Marketing. Sword and the Script. Retrieved from swordandthescript.com/2020/04/effective-thought-leadership/

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!

What do we call a collection of two or more computers that are located within a limited distance of each other and that are connected to each other directly or indirectly?

A) Internet
B) Intranet
C) Local Area Network
D) Wide Area Network

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