2180 Satellite Blvd
Suite 400
Duluth, GA 30097

Office: 877.468.1230

VectorChoice.com

TECHNOLOGY TIMES

INSIDER TIPS TO HELP YOUR BUSINESS RUN FASTER, MORE EFFICIENTLY, AND ULTIMATELY, MORE PROFITABLY

SEPTEMBER 2019

YOU ARE THE #1 TARGET FOR CYBERCRIMINALS TO HACK YOUR NETWORK …
AND WHAT YOU CAN DO TO PREVENT IT

"As a business owner, you don't have time to waste on technical and operational issues. That's where we come in! Call us and put an end to your IT problems finally and forever!"

Will Nobles
Founder & CEO
Vector Choice

Did you know that small businesses are more likely to be targeted by cybercriminals than any other business or organization? It's true! While we hear about major breaches on the news, we don't get to hear the stories of the businesses that struggle with hacking attempts and cyber-attacks.

Hackers love to go after small businesses for one very big reason: small businesses are less likely to invest in top-notch (or even worthwhile) cyber security. Hackers love this vulnerability.

According to the Verizon 2019 Data Breach Investigations Report, 43% of cyber-attacks hit small businesses. The reason comes down to many factors, but there are two in particular that hackers really dig into when going after targets: lack of resources and lack of knowledge. Of course, there's more to this story, as hackers also look at a business's customer base and the type of data the business shares online.

A lot of small businesses are also relying more on the cloud (and this is the trend moving forward), but then they do little to keep their line of communication with the cloud storage, or just the cloud storage itself, secure. According to Symantec, a lot of businesses that rely on the cloud also fail to rely on strong encryption software. They just share their data to the cloud and let that be that.

Hackers attack small businesses because they want money. Hackers go after targets they can profit from, whether they hold a business's data hostage and demand a ransom (and get that ransom – hackers got $460,000 from Lake City, Florida, officials after a ransomware attack on government computers, and that wasn't the only Florida city to pay!), or by stealing customer data and either selling it on

INSIDE THIS ISSUE

INDUSTRY UPDATE

5 TECHNOLOGY TRENDS YOU CANNOT IGNORE

Internet of Things (IoT) From WiFi-connected thermostats to smart locks, we're surrounded by IoT devices. Smart locks, for instance, can track who comes and goes. Mobile card readers eliminate the need for traditional cash registers.

Artificial Intelligence (AI) AI can enhance customer experience. For example, automate more of what you do on social media with the help of AI. It's getting better at delivering personalized experiences to customers. It's more time for you.

Telecommuting. Working between home and office easier than ever, and more employees are opting to use their own devices, saving the company big dollars. Plus, cloud collaboration has become simpler or more user-friendly.

Customer-Relationship Management (CRM) Software It's all about building and managing customer relationships. CRM is crucial in tracking prospects, logging e-mails and phone calls and more.

Voice Search More people are using assistants like Alexa and Siri to access information, including internet search. Optimize your SEO to get the most out of voice search. *TechRepublic, May 21, 2019*

IMPLEMENT THESE 2 STEPS NOW TO PREVENT FRAUD IN YOUR BANK ACCOUNT

Did you know your company's bank account doesn't enjoy the same protections as a personal bank account when it comes to fraud? If a hacker takes money from your business account, the bank is NOT responsible for replacing funds. Ask your bank what their policy is on refunding money stolen from your account! Many people erroneously believe the FDIC protects you from fraud. It does not; it only protects you from bank insolvency.

Tip: *Step 1:* Invest in insurance to protect you from fraud. *Step 2:* Set up e-mail alerts to receive notifications any time money is withdrawn from your account. You can also set it to alert you only for larger withdrawals. The *faster* you catch fraudulent activity, the better your chances are of keeping your money. If you contact the bank immediately after any money is taken out, you have a very high probability of stopping hackers from robbing you.

4 PROVEN TECHNIQUES TO IMPROVE PROJECT MANAGEMENT IN YOUR BUSINESS

1. Know the project's purpose/scope/goal. This is how you get focused. When you know your purpose, you can tackle the project one step at a time and not take a scattershot approach. It makes it easier to tackle as a team.

2. Set deadlines and budgets for every step. Give yourself a timeline for every step of the project to keep things moving. A budget can also help you delegate and spend accordingly. Deadlines and budgets also keep you more accountable.

3. Keep everyone looped in. Everyone on the project needs to know exactly what is going on. Everyone needs to be open on tasking, status updates and any scheduling. When you're all on the same page, things move along so much easier. Even better, use a web app to post everything into.

4. Review the project. Examine what went well and what didn't. Then, you can adjustment the next project and hammer down what worked while avoiding the same mistakes. *Small Business Trends, June 18, 2019*

the dark web or black market, or using it for themselves.

The Verizon report also looked at the types of businesses that are targeting. The top three are:

- Public administration (23,399 reported incidents and 330 confirmed data disclosure)
- Information services (1,094 reported incidents and 155 confirmed data disclosure)
- Financial and insurance (927 reported incidents and 207 confirmed data disclosure)

They go after these types of businesses because this is where they can make their money – and it's where they've discovered the most vulnerability. However, while these types of businesses represent the top three, there are many more. Every type of business is targeted. Some businesses make it past the attack unscathed, but many don't. Their data is compromised in one way or another.

Why are small businesses are targeted so much? It's a numbers game. Hackers know most small businesses lack good cyber security. This makes these businesses easier targets. Target enough of them, and you're going to make some serious money (from selling stolen data or paid ransoms).

So, what can you do about this? How can you protect your network? First and foremost, you have to realize YOU are a target. It doesn't matter if you've never been hacked before. It just means the hackers haven't gotten to you yet. Once you realize this, you can go to work and get your business ready for the eventual attack.

his is where a risk assessment can do a lot of good. You may already have some security measures in place, but do you know how effective those measures are? You need to know where your holes are so you can plug them and then reinforce them. You don't want just a wall around your business, you want an entire ocean.

But it doesn't end there. One of the most powerful tools against hackers and cybercriminals is knowledge. Next to securing your business, the best thing you can do is train your employees on understanding cyber security and the threats that exist to harm the business they work for. Your team MUST know how to identify phishing schemes, fraudulent websites and virus scams, then stay regularly updated on the threats out there. (And don't forget using complex passwords that are locked away in a password vault or manager to add another layer of security).
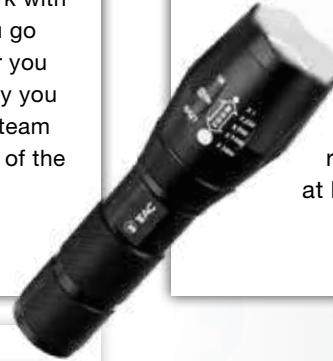
On top of this, work with an IT team who knows what they're doing. It's one thing to tackle this all by yourself, as many businesses do, but it's another to work with an experienced IT security firm. If you go it alone, you might miss something or you might not fully understand the security you have in place. Having an outsourced team of pros means you're one step ahead of the hackers.

VECTOR CHOICE NEWS

TRIVIA

Who wants to win a $25 gift card?

You can be the 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!

These keys were originally programmed to always send the same signal/code. However, which of these set of keys can now have a different instruction set for every operating system and/or application?

A. Number keys   C. Direction keys

B. Lock keys   D. Function keys

Ready? Call us right now with your answer!
877.468.1230