TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

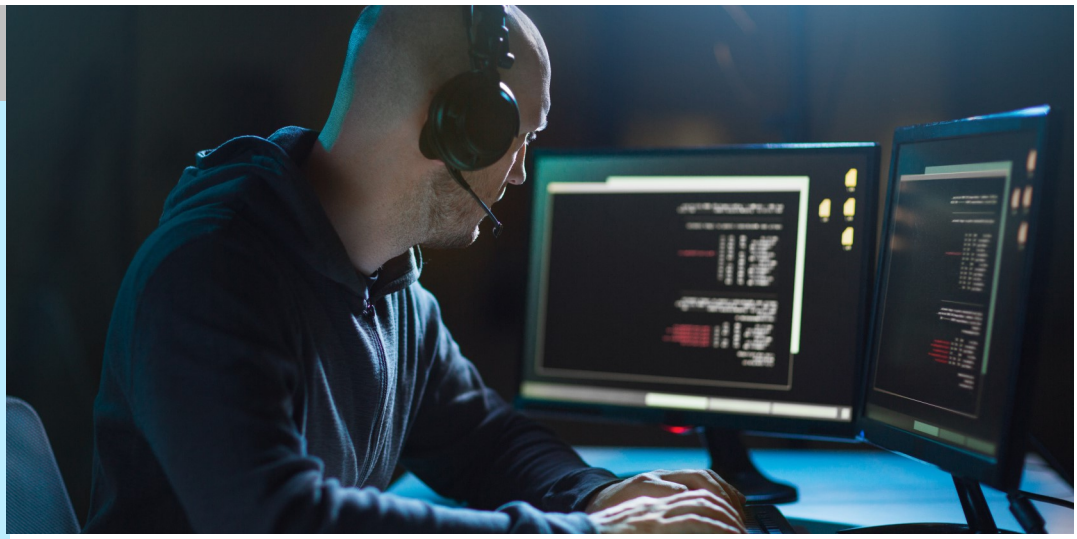
What's New

Lorem ipsum dolor sit amet, periculis signiferumque eu usu. Homero pertinacia mel ea, cu qui vero contentiones. Per postea voluptua ad, aperiam senserit instructior an usu. Te modo vocibus mel, id eam eros qualisque. Eum enim habeo ne, mea et audiam mnesarchum.

Movet fierent voluptatum no vis, sea principes argumentum ei, ut eros zril delicatissimi nam. Laudem ridens vituperata eum ex. Vim graeco philosophia concludaturque cu, at pro semper perpetua noluisse.

July 2020

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



3 Critical Cyber Security Protections EVERY Business Must Have In Place NOW To Avoid Being Hacked

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 were set. But then you forgot to do one crucial thing: you didn't stay up-to-date with your IT security policy.

This is a trap countless businesses fall into. They invest in great cyber security *once*. Five years ago, this was fantastic. The problem is that cyberthreats are constantly 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 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

Continued on pg.2

Continued from pg.1

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.

This is why you need a cyber security handbook – 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. This helps keep your employees from becoming the weak link in your security setup.

Update, Update And 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 a piece of hardware (like a router) is no longer supported by the manufacturer? This occurs 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.

"Proactive monitoring means your network is being watched 24/7."

You might balk at the cost of buying new technology, but in the long run, the cost is well worth it. Think of the cost of buying a new router versus the cost of 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. Proactive monitoring means your network is being watched 24/7. Every little ping or access to your network is watched and assessed. If a threat is found, then it can be stopped.

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 can be done too! This approach means you have one less thing to think about. 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 be updated 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 Technology Truths For Transforming Your Business

1. You have to keep up. Tech changes fast. By the end of this year, 5G will be more widely available – along with devices that can use it. More businesses will be relying on artificial intelligence to supplement productivity and customer interaction, putting them light-years ahead of the competition that lags behind.

2. You have to invest. Change comes with cost. If you aren't willing to invest in new tech, then you will fall behind, and so will your support and security. If you run into any problems, then you could be in big trouble.

3. Don't fall behind on cyber security. It's easy to forget about cyber security when things are running smoothly and working as intended. But cybercriminals never stop. They are always looking for a way in, and if you fall behind the times on your IT security, then you make it easier for them. Keep your data and your customers as secure as possible. *Inc., July 30, 2019*

How Malware Can Cripple Your Business

Every year, the number of malware attacks on small businesses increases. Semantec's 2018 Internet Security Threat Report found that between 2017 and 2018, malware increased by 54%.

The term "malware" covers a number of different malicious programs, including ransomware, spyware, viruses, worms, Trojan horses and more.

In many cases, malware is designed to take over your computer. It may be programmed to look for specific data or it may give a hacker remote access to your files. In the case of ransomware, it locks you out of your computer until you pay the hacker a ransom. After that, the hacker may give you back control – or they might delete everything on your hard drive. These are not good people.

If you don't invest in cyber security, then hackers can destroy your business. It's already happened to countless businesses across the country. It's estimated that websites experience up to 58 cyber-attacks every day. Protect yourself before it's too late. *Small Business Trends, Oct. 12, 2019*