two river™
TECHNOLOGY TIMES

What's New

Is Your Data Secure?

In today's culture, data security is more important than ever. It would be horrific for many if their personal information was compromised. Unfortunately, your data may not be anywhere near as secure as you might hope.

The Pegasus Project is an exposé that revealed that a piece of spyware can exploit a user's Apple or Android devices to take control of the user's device. A list of 50,000 victims was published that included government officials, business executives and royal family members – proving that nobody is safe.

Tech companies usually write extremely secure codes initially, but as new features roll out, holes are created in the defense that hackers can exploit. Pegasus proved that, in the software world, if an adversary is well-motivated, they will find a way in.

The key to staying protected from these breaches is depth. Multiple lines of defense are more protective, so don't stop at one. Though one security tech may have plenty of gaps, another could fill those and strengthen your security.

New security technologies are continuing to advance the security field. There are plenty of actions you can take to ensure that your data remains secure.

November 2021

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

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

A Proven Method To Secure Your Business's Network

People don't usually think about small businesses when discussing cyber security. The media covers breaches in governmental and big-business security in excess. These entities usually have lucrative targets that attract the attention of hackers but are often backed up with an extremely protective network security system that's difficult to crack. When hackers can't break the big system, they turn their attention to easier targets.

While most hackers want the opportunity to crack a high-risk target, these situations are few and far between. Instead, they turn their attention toward much lower-hanging fruit. This is where small businesses come in; they still have access to money and data but have much lower defense than a governmental entity. Luckily, many average cyber security strategies can keep the would-be hackers away. Their methods are always changing, though, and it helps to be one step ahead of the game. These are the best current cyber security strategies you can put into place.

Cloud Security

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage and deletion. As more and more businesses switch from hard-drive data storage to remote databases, this practice is becoming more and more commonplace. Methods of providing cloud security include firewalls, penetration testing and virtual private networks (VPN), to name a few. While many people feel that their data and information are better stored on a hard drive on their own network, data stored in the cloud may actually be more secure, depending on the system's defense strategy. Be wary, though: not all cloud securities are made the same. Do your research and pick one that will best protect your data.

Continued on pg.2

Continued from pg.1

Network Security
Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse or theft. This is what your network administrator will need to put into place in order to keep your devices and data secure. The best approach to protecting your network is to create a strong WiFi password. Random numbers and letters work best for a small business since nobody but those who need it will be able to guess the password. In addition to a strong password, you'll also have to anticipate any type of internal attack.

VPNs And Firewalls
A VPN can help protect your security by masking your IP address. This essentially means that you'll be connected through a different server, making it much harder for the government or websites to pinpoint your location. It also encrypts all network data by creating a secure tunnel.

"Many average cyber security strategies can keep the would-be hackers away."

A firewall is simply a shield that protects your computer from the Internet. Firewalls can help restrict access to sites that could be damaging to your network. Both of these tools can be highly effective when used properly, but they do not protect against all threats.

Updates And Upgrades
While it might seem simple, consistently updating and upgrading your technology tools can keep you much more secure. The developers of many of these tools are constantly looking for new threats that pose a risk to their program. They'll issue patches to make sure any holes are filled. You just need to make sure that all of your tools are updated in a timely manner and verify that the updates are installing.

Data Backups
You should always have multiple backups of your business's data. You never know when a power surge or some type of natural disaster might cause your current files to be deleted. You can prevent this issue by regularly backing up your data.

Employee Training
It's important to limit employee access to systems and data owned by your company. Not everyone needs to have access, so only give it to those who can't work without it. There should also be some type of security training for all employees. Phishing schemes and weak passwords create just as many issues as hackers do. Finally, you should make sure everyone in your workplace is security-conscious. A single breach could critically hurt your business. Your employees need to understand this so they can be proactive as well.

No matter which route you take, the most important thing you can do for your small business is protect its network. Governmental entities and big businesses do not suffer from security lapses nearly as bad as small businesses. A security lapse could even stop your business dead in its tracks.

Free Report Download: If You Are Considering Cloud Computing For Your Company, DON'T, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report: **"5 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."**

This report discusses in simple, nontechnical terms the pros and cons of cloud computing, data security, how to choose a cloud provider and three little-known facts that most IT consultants don't know or won't tell you about cloud computing that could end up causing you MORE problems and costing you more money than you anticipated. **Even if you aren't ready to move to the cloud yet**, this report will give you the right information and questions to ask when the time comes.

To receive a copy of this FREE report, email kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

Angel Guard Cookware Prevents Burns

Many people burn themselves every day while cooking in their kitchens. There's a new product on the market that aims to prevent these injuries. After firefighter Eric Le Blanc responded to back-to-back kitchen burns involving children, he knew there had to be a safer alternative. In his research, he found that tipping pots of hot liquid were the world's leading cause of adolescent burns.

Le Blanc developed the world's first tip-proof cookware: Angel Guard Cookware. This cookware removes risk by including a removable stem that slides underneath the burner grate and locks the cookware into place. Now parents no longer have to worry about their child getting hurt after removing a pot from the stove.

Hiring The Best Staff

Not long ago, I had the opportunity to sit down with Carter Cast, the author behind *The Right – And Wrong – Stuff: How Brilliant Careers Are Made And Unmade*. Hiring success has a great influence on career success, and we discussed five negative archetypes that confront employers while filling a job opening. Together, we discovered some telltale signs that your interviewee may fall into one of these categories.

Captain Fantastic
While it might seem like "Captain Fantastic" would be a vital part of your team, they often cause division. Someone who is a "Captain Fantastic" is usually overambitious and has no qualms about stepping on others to get ahead. If you're interviewing a candidate and they mention that their greatest accomplishments revolve around beating others rather than delivering value or developing teams, you probably have a "Captain Fantastic" on your hands.

Solo Flier
Have you ever worked with someone who thinks their way is the best and only way to do something? It's very frustrating. While this type works well individually, they can be detrimental to a team environment. They usually claim to have no time or were too busy to accomplish their tasks; in reality, they may fail to hire and delegate properly. I've met with many people who fit this category and end up leaving their job due to burnout after taking on too much work.

Version 1.0
Change is a necessity in the workplace, but sometimes, people prefer to stick to their routine. To spot these people in interviews, listen to their stories and pay attention if they mention changes in the workplace and how they responded. If they stayed on the same path, that's a red flag. I knew a manufacturing executive who failed to adapt to new technologies. This caused him to lose some of his biggest clients, and the business fell into a tailspin.

The One-Trick Pony
These people usually get stuck in a rut because they rely on their greatest strength to solve *all* problems. They will often aim for lateral moves rather than trying to broaden their horizons. I interviewed a one-trick pony recently who wrote amazing copy but struggled when meeting with clients face-to-face. His communication skills weren't strong enough to work with clients or lead large teams. His career became stagnant even though he was eager to grow and move up.

Whirling Dervish
Energetic employees improve morale and production in a workplace, but sometimes lack the follow-through needed to complete projects. You can usually spot these people in interviews if you notice them avoiding your questions. They often come up with excuses for why they didn't achieve results. Great ideas and strong morale do not make up for a lack of completion.

With knowledge of these archetypes, you can avoid hiring the wrong candidate for your team and instead focus on finding the perfect fit.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times *best-sellers. He stays active in his community and has advised many government officials.*

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

TRTG Happenings

Scam of the Month

Katie wanted to help and donate to the earthquake relief efforts. She searched "Earthquake Donation" on her favorite social media site and clicked on a crowdfunding page that asked her to provide her credit card information, address, and other personal details. The page then mentioned she could be eligible for tax credits but needed to enter her Social Security number, which she did. The next day her bank called to report the suspicious activity. They were able to reverse her original donation, but her exposed Social Security number put her in grave danger of future scams. She needed to put a credit freeze on her account which inhibited her from purchasing her dream home.

- Katie searched for a charity on social media and selected a crowd funding page.
- Katie gave out far too much information in the online form.
- Katie failed to do any research to determine if this charity was reputable or not.

Charity scams have become very common, especially after natural disasters that make the news or during the holiday season when the giving spirit is in full swing. Be cautious with crowdfunding pages and do your research. While there are many reputable charities that are responsible with their donations, there are others that were created by scammers with the sole purpose of stealing information and funds from generous givers.

Along with fake web pages, watch for unsolicited phone calls, as well. Scammers commonly pose as reputable charities to collect your donation quickly over the phone. Beware of pressure tactics by the caller encouraging you to act now. Try hanging up and visiting the charity's website directly to donate securely or use a charity verification resource that may be provided by the government.

Make sure your money gets to the people that need it the most. Be diligent about researching reputable charities to make sure you are donating securely.

Dispose of Your Electronics Wisely

Getting rid of old computers or servers? Did you know that the components used in technology equipment are not landfill-safe? On top of the environmental hazards, unprotected e-waste typically contains a lot of confidential and private information in the form of saved passwords, Internet history and files left on the retired computer or server.

As a first prevention step, find a local recycling facility where e-waste can be safely disposed of. And make sure to take the following #1 security precaution before you haul it off: remove and destroy the hard drives. A drill and hammer usually do the trick just fine. Alternatively, many companies that shred paper documents will also destroy your hard drives.

We offer free e-waste recycling services to our clients – just let us know and we'll pick up your old hardware and make sure it's properly recycled.

Don't forget other e-waste such as mobile phones, copy machines and any other device that ever touched your company data. Give serious thought to what data is on any device before you recycle it.

two river™
TECHNOLOGY GROUP

TESTIMONIAL

"I always call you when things are broke. I just want to note that things are great and knowing you are out there is comforting. Thank you for all you and the team at Two River does."

-Al Procaccino II
Castle Financial