The Tech chronicle

What's New

FREE

Executive Seminar

"7 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber-Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

Register Online At:
https://www.vertech.co.nz/securityseminar/?cl

Or Call Us At 020 4016 7246
See Pg. 5 for more details

Please be my VIP Guest for this upcoming executive session." -

Daniel Watson, Vertech IT Services

February 2020

Our Mission:
We support and protect the dynamic owners of growing businesses allowing them to scale by providing Stable, Secure and Scalable IT Services & Solutions.

We aim to be the first choice as a Trusted IT Partner for these businesses on the North Shore & Auckland

vertech IT SERVICES

Top 3 Ways Hackers Will Attack Your Network — And They Are Targeting You RIGHT NOW

You might read the headline of this article and think, "That has to be an exaggeration." Unfortunately, it's not. Every single day, small businesses are targeted by cybercriminals. These criminals look for vulnerable victims, then attack.

This is the world we live in today. It's one where cybercriminals regularly take advantage of small businesses. Why small businesses? They're the favorite target of hackers, scammers and other cybercriminals because small businesses have a bad habit of NOT investing in cyber security.

Hackers have many methods they use to break into your network, steal data or put you in a position where you have to pay them money to get your data back. They use a combination of software and skill to make it happen. Here are three ways hackers and cybercriminals attack your network in an attempt to get what they want.

1. THEY GO THROUGH YOUR EMPLOYEES.
That's right, they'll use your own employees against you, and your employees might not even realize what's happening. Let's say a hacker gets ahold of your internal e-mail list, like the e-mails you have posted on your website or LinkedIn. All the hacker has to do is send an e-mail to everyone at your company.
The e-mail might be disguised as a message addressed from you asking your employees for a gift card, which is becoming an increasingly common scam. Another e-mail tactic is making a message look like it's from a fellow employee, asking everyone else to

Continued on pg.2

Continued from pg.1

open an attached file, which is likely malware or ransomware. A third e-mail scam is directing people to a phishing website, which is a website that scammers have designed to look like popular websites in order to get login information to hack accounts. All it takes is a single click from any employee to let the bad guys into your business.

2. THEY ATTACK YOUR NETWORK DIRECTLY.
Some hackers aren't afraid of forced entry. Hackers and cybercriminals have access to black market tools and software that helps them get into networked devices – particularly *unprotected* networked devices.

For example, if you have a PC that's connected to the Internet and your network doesn't use any firewalls, data encryption or other network protection software, a hacker can break in and steal data from that PC and potentially other devices connected to that PC, such as portable hard drives. This method of entry isn't necessarily easy for hackers, but the effort can be worth it, especially if they can walk away with sensitive financial information.

3. THEY HOLD YOUR DATA HOSTAGE.
Hackers are relying on ransomware more and more to get what they want. Hackers rely on e-mail, executable files and fraudulent web ads (such as banner ads and popups) to attack networks with ransomware. It goes back to the first point. All it takes is someone clicking a bad link or file and the next thing you know, you're locked out of your network.

This has happened to dozens of businesses and even city governments in the last year alone. The thing is that even if you pay the ransom, there is no guarantee the hacker will restore access. They can take the money and delete everything, leaving your business high and dry! This destroys businesses!

All of these points are why you need to take a hard look at IT security solutions *and use them.* For instance, if you had all of your data *securely* backed up to the cloud and a hacker came in and tried to hold your data hostage, you wouldn't have to worry. They don't really have your data. You can tell them "no," then all you'd have to do is work with an IT team to get your network back up and running while scrubbing it of any malware or ransomware. Then, it would be a simple matter of restoring data from the cloud. Sure, you might be out of commission for a day or two, but in the grand scheme of things, it's *much* better than losing your business to these jokers.

Hackers are just looking for easy targets and, sadly, a lot of small businesses fit the bill. Just because you haven't had any major problems yet doesn't mean you won't in the future. The threats are out there and they're not going to go away. Invest in security, partner with an IT security firm and protect yourself. This is one investment that is truly worth it!

"Hackers are just looking for easy targets and, sadly, a lot of small businesses fit the bill."

Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment (valued @ $540) now, call our office at 09 972 0367

Client Spotlight

Mortgage Link (NZ) Limited was established in 1991 as a Mortgage aggregator business. It now has representation in 40 plus locations nationally with +- 130 advisers representing both Mortgage Link and its younger sister company Insurance Link.

Mortgage Link is 100% New Zealand owned and operated and is proud of the fact that we've helped thousands of kiwis with home financing and related needs for almost 3 decades.

Building on from its founding principles Mortgage Link is committed to providing quality service to its clients.

The prime objective is to provide clients with a comprehensive but tailored approach to lending and insurance taking into account client's specific personal circumstances and motivations, in order to arrive at an individualised recommendation.

Mortgage Link provides its advisers with branded as well as non branded options, compliance support, ongoing training and development, networking opportunities and Promotions.

Josh Bronkhorst
Managing Director
Mortgage Link

www.mortgagelink.co.nz

The First Mistake Bad Leaders Make In A New Job

The first mistake bad leaders make in a new job is subtle, common and avoidable: they come into an organization and they don't narrow the priority list.

In our research for *Power Score*, we found that only 24% of leaders are good at prioritizing. And when a leader is bad at prioritizing, 90% of the time it's because they let too many priorities stay alive.

In short, great leaders **prune priorities**.

What does priority pruning look like?

It looks like taking a weed whacker to the overgrown mass of useless priorities that grow inside organizations.

It looks like what Steve Jobs did when he returned to Apple and trimmed the number of products from hundreds to under 10.

It looks like what In-N-Out Burger (for those of you who have enjoyed this delicious West Coast treat) does in only giving you a menu of burger, fries and a drink.

It looks like what Scott Cook, founder of Intuit, did in making QuickBooks as easy as using your checkbook.

There are so many leaders I see who lack the analytical horsepower, the courage or the decisiveness to prune priorities, so they just let dozens, hundreds or even thousands of priorities live on in their organizations and distract people away from the small set of things that matter most.

If you want a simple way to prune priorities, use the one-page discussion guide straight out of our *Power Score* book. Have your team rate your priorities 1–10. If you are scoring a nine or 10, keep doing what you are doing. If you score less than a nine, then it's time to get out the weed whacker!

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times *best-selling book,* Who: A Method For Hiring, *and the author of the No. 1* Wall Street Journal *best seller* Leadocracy: Hiring More Great Leaders (Like You) Into Government. *Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring, and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with honors from Northwestern University, and an MA and PhD in Psychology from Claremont Graduate University.*

Top Ways To Protect Your Remote Employees From Cyberthreats

Allowing employees to work remotely comes with its share of benefits, like increased productivity and employee happiness. But it comes with challenges as well, including staying ahead of cyberthreats. Here are three ways to protect remote employees who work from laptops, tablets and smartphones.

1. Avoid unsecured public WiFi. It may be convenient, but cybercriminals can use unsecured networks to steal data. Instead, remote workers should utilize a virtual private network (VPN). Personal hotspots are another option.

2. Require endpoint security, such as firewalls and malware protection, installed on remote workers' devices. All remote employees should use the same endpoint security so you know everything is up-to-date.

3. Develop 'cyber security best practices' for your business. Everyone, including remote workers, should be on the same page when it comes to cyber security. Make sure your employees know the threats and how to stay vigilant online. *Inc., Feb. 12, 2019*

6 Ways To Make Your Business More Efficient

1. Cut the clutter. Have any outdated systems and processes that are cluttering up your business? Get rid of them. Look for inefficiencies or redundancies you can eliminate, then do it!

2. Block interruptions. When you need to work, it's okay to put up barriers. Block out your calendar when you don't want calls. Turn off all phone notifications. Only check e-mail twice a day. Set limits!

3. Look to automation. Whether you're scheduling e-mails or social media posts, look at what you can automate to avoid wasting time.

4. Balance tech and traditional. It's okay to rely on texting, e-mail and online chat to communicate with customers, but don't forget the power of real, face-to-face communication.

5. Say no to multitasking. Multitasking is a myth. You can either do several things at once and deliver mediocre results or do one thing right the first time and deliver stellar results.

6. Invest more in cyber security. There are countless threats out there, so don't get caught without good IT security across the whole of your business. Don't risk it! *Small Business Trends, Nov. 4, 2019*

3 Simple Ways Introverts Leverage Their Strengths To Thrive In The Workplace

Introverts can be drained by social interaction and stimulation. They need to recharge regularly, so days off are important in order for them to be at their most productive. Here are three ways introverts can be at their best in the workplace:

- Manage energy more than your time. When you feel most energized, that's the right time to focus on creative work that requires more brainpower. Structure your days around your energy.
- Cultivate the right environment. Work in a space that calms you and energizes you. Set the right light (such as natural lighting) and invest in noise-canceling headphones.
- Say what needs to be said. Introverts constantly think but don't always speak up. Don't let communication fall to the wayside. Remember, we're all working together. *Business Insider, Nov. 19, 2019*

vertech IT SERVICES

Please be my VIP Guest for this upcoming executive session." -

Daniel Watson,
Vertech IT Services

During This Must-Attend Seminar You'll Discover:

- **The scary risks of mobile and cloud computing - and 7 critical policies, procedures and protections EVERY business must have in place NOW to protect themselves**; overlook even one and you're exposing yourself to security breaches, damaging and expensive litigation, employment lawsuits and having confidential company information exposed to competitors, hackers and cybercriminals.
- The **#1 security threat to your business** that anti-virus, firewalls and other security protocols are defenseless against.
- A **SHOCKING truth about bank fraud** that most businesses don't know about that could (literally) wipe out your bank account.
- **Why firewalls and antivirus software give you a false sense of security** - and what it REALLY takes to protect your organization against new threats and today's sophisticated cybercrime rings.

FREE

Executive Seminar

"7 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber-Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

Event Details:

When: 19 March 2020

Time: 12:30 p.m.—13:30 p.m.
13:30 p.m.—14:00 p.m.

Where: The Crate
28 Constellation Drive
Albany
Auckland, 0632

Register Online At:

https://www.vertech.co.nz/securityseminar

Or Call Us At 020 4016 7246

Who Should Attend?

Managing Directors and Business owners who are concerned about: lost or stolen devices, privacy of confidential information, employment litigation introduced when employees use personal devices to access company data, and the proposed New Zealand legislation on cybersecurity breach notifications for lost or stolen data. This is of particular importance for those organizations that handle ANY sensitive data such as credit card and financial information, medical records (or serve clients who have medical records) or that simply want to avoid having their bank account wiped out due to a cyber-attack.