Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"
Since 1984

Hackers Don't Take Vacation

Hackers don't take a vacation, but they're excited for you to take a summer vacation! They're eagerly awaiting you and your team to become more relaxed about cybersecurity during the summer months.

When you're traveling, it's far more likely for you to connect to an unsecure network or take a shortcut that would leave your computer and company more vulnerable to a cyber attack. When members of your team are on vacation, other team members are covering their daily tasks. This means they could become more distracted and make a mistake like clicking on a link in a phishing email.

Please remember this summer to keep cybersecurity in mind as you and your team travel and enjoy your summer activities. Hackers are just waiting on the sidelines for people to get distracted and complacent.

June 2022

This monthly publication provided courtesy of Ryan Haislar, President of Computerease.

"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!"

How A Phone Call Prevents You From Mistakenly Sending Money To A Hacker's Bank Account

It's easier than you think to electronically transfer your business's hard-earned money directly into a hacker's bank account. The most insidious thing is that your business and technology don't even need to be hacked! If one of your vendors gets hacked, you are a prime target because of your established relationship with that vendor.

Would your team send money directly to cyber criminals if your vendor gets hacked?

It all depends on your financial department and its policies for vendors and bank transfers. Imagine this scenario. You've been working with a vendor for 10 years and regularly interact with your main contact there. One day you get an email from that person asking you to update the bank account information where you send regular ACH payments. The email address looks the same, the tone and wording of the email is the same, and the email signature is the same. They might even include something you have previously discussed.

Be Suspicious of Email Requests

If you update the banking information for a vendor based solely on an email, you could be falling right into the hacker's trap. The updated banking information could be a bank account for a cyber-criminal ring that's hacked into your vendor's email account. They could have been going through a person's inbox, unnoticed, seeing all the email interactions with you and other companies.

All it would take is one carefully crafted email sent from an almost identical email account to trick you into voluntarily updating the

legitimate bank account information to the hacker's bank account. It's most common for hackers to create a spoofed email account with a new domain that's almost indistinguishable from the legitimate domain. A minor spelling variation is all it takes. For example, microsotf.com instead of microsoft.com. If you aren't intentionally looking for a spelling mistake, you won't notice the difference.

Money Lost Without Knowing

How long would it take to notice if your team was unwittingly paying hackers instead of your vendor? Most likely, the vendor would reach out for non-payment after a certain period. It's not uncommon for a vendor to reach out after a few months. In that time, thousands or hundreds of thousands of dollars can be siphoned out of your business accounts, sent directly to hackers.

Making a Phone Call to Verify

There's a much better possibility, a simple phone call, that will stop the hackers in their tracks. A phone call verification to the contact person at your vendor to confirm that there is a legitimate need to update their bank account information. ***The key is to only call a known good and authentic phone number!***

A hacker can easily put a fraudulent phone number into an email signature and impersonate the vendor and contact information, so it's essential to verify the phone number. Only call a phone number you can verify is legitimate from other means!

People Are the Biggest Cybersecurity Risk

Hackers are experts at two things – finding vulnerabilities in technology and tricking people. It's a great day for a hacker when they can trick a person into clicking a link, sharing sensitive information, or being lax about following recommended security protocols. It's a very bad day for you and your business when this happens.

Every cybersecurity strategy needs to include protections for both technology and human vulnerabilities.

- Require cybersecurity training for your entire team
- Address cybersecurity risks in your day-to-day operations - assuming your team WILL make a mistake at some point
- Conduct an annual cybersecurity risk assessment
- Implement and utilize multi-layered cyber security protections
    - o Make sure your business email isn't hacked by mandating two factor authentication (2FA) for all email accounts – your business could have its emails spoofed and you could be the vendor held liable in this scenario
- Obtain cyber liability insurance in case the worst does happen

Security Strategies for Every Aspect of Business

With intention and thought, you can implement policies and processes that make a hacker's job harder. You can train your team to be aware of warning signs of malicious emails while also applying processes to double-check for human error. A perfect example of this safeguard is adding in a phone call whenever a vendor requests an update to bank account information. It will take 5 minutes at most and save you thousands of your hard-earned dollars.

Many business owners think they have reasonable cyber security protections in place. However, they underestimate hacker's innovative methods and sheer determination to gain access to their business email and technology systems. The Computerease team helps our clients understand and manage cyber security risks in every aspect of their businesses through both training and technology.

If you need help, give us a call and we can help protect your business from hackers.

Free Email Phishing Test: Who will take the bait and put your company at risk?

Over 90% of cyberattacks start with an email! Take proactive steps to educate your entire organization about the signs, the risks, and the disastrous outcome of email phishing attacks.

- Make employees aware of the risks of email phishing attacks
- Real-life cybersecurity training your employees won't forget
- Learn which employees fall victim to the simulated phishing email
- Provide additional training to employees who need it most

Claim your FREE Email Phishing Test Today At:
www.computer-service.com/phishing-test

Shiny New Gadget Of The Month:

NeckRelax

Do you spend a lot of time hunched over your computer at work? Many people work on their computers for multiple hours a day and start to develop pain and stiffness in their necks because of it. While you can get a prescription to manage the pain or try to get a massage, these options aren't appealing to everyone. NeckRelax is the newest neck pain relief tool on the market and is working wonders for people who are using it. NeckRelax offers six distinct massage modes and infrared heat and also comes with a set of electrode pads to target specific muscles. NeckRelax sells for $119 but often goes on sale on their website: NeckRelax.io.

Get out of pain and take back your life with NeckRelax.

3 Ways To Get Your Life Back

When first starting out in my career, I had a meeting with an executive where I worked that completely revolutionized how I viewed things. While sitting in her office, I noticed a small picture frame on her desk that had a note with the words "eat lunch" on it. I asked her why she had that sign, and she responded by saying that she'd become too busy to eat lunch most days. This scene absolutely horrified me. Work is not supposed to suck the life out of you.

After this experience, I decided to never be in a similar situation, and I wanted to make an effort to ensure that other business leaders never felt like their work controlled every aspect of their lives. I developed three ways for business leaders to reclaim their lives. While doing each one will help in its own way, in order to truly get your life back, you need to do all three.

The first thing you need to do is make personal goals. We're always setting new goals when it comes to our businesses, but we also need to have goals for our everyday lives. These goals must line up with what you want to do when you're away from the office. I know of one CEO who set a goal to be at home when his teenager was off from school at least four days a week. Figure out what you want to accomplish at home or with your family, and make the necessary changes to ensure that reality.

Just setting goals might not be enough. You also need to schedule personal time. I called one of my colleagues recently, and when he answered, he asked a question about a diaper bag. I felt confused by this at first, but he clarified that he had taken the morning off to bring his family to the zoo since the kids returned to school the next day. Always leave time for yourself and your family. If somebody is trying to schedule your time over one of your personal commitments, tell them you are not available.

The final way to reclaim your personal life is the "delete, delegate, delay and do" method. When you first get a task, just don't do it and delete it. If it's too high of a priority, see if you can delegate it to someone else. If there's nobody to delegate to, see if you can delay. If that's not practical, then just do it.

If you follow these three tactics, you'll see positive results in your personal and professional lives.

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.

3 Big Technology Trends For Businesses In 2022

Many of the changes brought forth by the pandemic are here to stay and may even evolve further. The year 2022 is shaping up to be a big one for technology, and you'll want to stay informed if you plan to keep up with any changes in your business.

With more people working remotely than ever before, there's been a greater focus on Internet speeds and usage. Over the next year, we'll experience an increase in 5G coverage as well as rapid development for 6G. Additionally, we're likely to see some growth in the AI sector. It's also imperative that you pay attention to the Metaverse and any impending developments, as the Metaverse has the potential to majorly impact a lot of industries.

Avoid These E-mail Marketing Tactics

E-mail marketing campaigns are performed by almost every company because they're a cost-effective way to reach a large number of potential customers. However, have you ever felt like your campaign was not getting the attention it deserves? Is it possible you did something that actually turned people away from your campaign? You'll want to reconsider your approach if you're doing any of the following:

- Using clickbait subject lines
- Using your e-mails only as a platform to sell
- Sending too many e-mails too often
- Failing to personalize any of your e-mails
- Focusing on company-related content instead of making it relatable

Get The Most Out Of Your Products

When you first start a business or develop a product, you're probably trying to figure out a way to maximize its value. Sometimes it's not enough to simply create a great product or service. You need to inject it with the spirit of your company. When you first started your business, you should have written out some core values you never want to forget. Your products should also follow these values and, at times, be the greatest representation of them. Oftentimes, you can showcase this through the design of the product itself and its packaging. When someone first uses your product or service, it should look flawless and work perfectly. When a potential customer first sees your product and uses it, they should have no qualms about the quality or design. They should view your product the same way you ideally view it – like it's the best thing since sliced bread.