Cyber Times

Newsletter by Secure ERP, Inc.

Insider Tips to Make Your Business Run Faster, Easier, and More Profitably

Email Theft Alert!

SC Magazine reports Business Email Compromise (BEC) surged 81% in 2022. What does that mean for your business?

Hackers are breaking into your email and may wait 6 months to spring changes on customers or even vendors ensuring the hackers receive your payments instead of you.

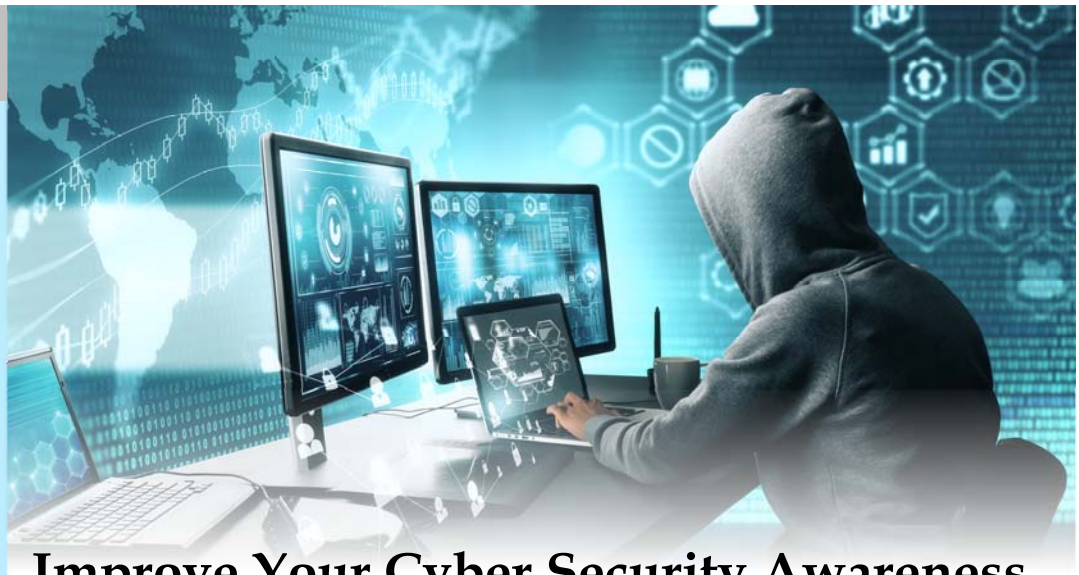
Victims lose MILLIONS of dollars this way. The FBI calls it the $43 Billion scam
www.ic3.gov/Media/Y2022/PSA220504

We can audit your email accounts and harden the protections so you aren't a victim. Call us for your audit.

March 2023

Too many businesses are exposed and vulnerable to cyber attacks. With a unique Guardian Angel Protection solution, our clients get back to their business and sleep better knowing their data is secure

This monthly publication is provided courtesy of Rick Rusch, CEO of Secure ERP, Inc.



Improve Your Cyber Security Awareness

Learn About Today's Most Common Types Of Cyber-Attacks

If you've turned on the news sometime during the past few years, you've probably heard of more than one instance where a business closed due to a cyber-attack. You may think your business is small enough and hackers won't target you, but this couldn't be further from the truth. Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats. With the right type of attack, a cybercriminal can gain valuable information about your business, customers and employees, which can be used to damage your reputation and hurt you financially.

If you're a business owner or leader and you want to ensure your business is well-protected, check out the most common cyber-attacks that are affecting companies today. From there, you can implement cyber security plans and tactics to ensure your business is protected from cybercriminals.

Phishing Scams
Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. Phishing scams can wreak havoc on your business and personal life. You may have seen an e-mail from someone claiming to be Amazon or your credit card company asking for specific sensitive information. Often, the e-mail address does not line up with who the person is claiming to be.

When a phishing scam targets your business, they'll likely request valuable information from your employees such as passwords or customer data. If your employees fall for the scam, they could give a cybercriminal unprecedented access to your network and systems. This may also allow the cybercriminal to steal private employee and customer information, leaving your employees

Continued on pg.2

Continued from pg.1

vulnerable to identity theft. Phishing scams can be averted by using common sense and providing cyber security training to your employees. Most companies will not request private information over e-mail. That being said, if an employee receives a suspicious e-mail, they should do their due diligence to ensure the e-mail is genuine before responding in any way.

Malware

Malware is software installed on a computer without the user's consent that performs malicious actions, such as stealing passwords or money. There are many types of malware, including spyware, viruses, ransomware and adware. You can accidentally download malware onto your computer by clicking on sketchy links within e-mails or websites. You might not even notice you have malware on your computer right now. If your computer is operating more slowly than usual, web browsers are taking you to random sites or you have frequent pop-ups, you should scan your computer for malware.

Prevention is key in stopping malware from affecting your business. Hiring and utilizing a managed services provider is the best way to protect your business, as they will continually monitor your network for exploitable holes. With malware, it's always better to play it safe than sorry. If a cybercriminal is able to use ransomware on your network, your business could be stuck at a standstill until you pay the ransom. Even if you can pay the ransom, your reputation will still take a hit, and your business could be greatly affected. Be careful where you click on your phone, too, since malware attacks on cellphones have become more common over the past few years.

Attacks Involving Passwords

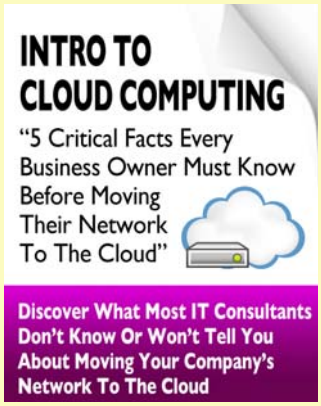
How do your employees access your network or computer systems? They most likely use a password to log in to their computer, access their e-mail and much more. What would happen if someone with bad intentions gained access to one of your employee's passwords? Depending on the individual's access, they could obtain sensitive information about your business, customers and employees.

Your team should be using long, complex passwords for their accounts, and each password for every account should be different. Encourage your employees to use password managers that will allow them to create the most complex passwords possible and keep track of them more easily. You can also incorporate multifactor authentication to ensure nobody can steal a password and gain access immediately. You should make your employees aware of this during your annual cyber security training.

If your business falls victim to a cyber-attack, it could have lasting consequences for everyone involved. Now that you know the most common types of cyber-attacks, you can start implementing plans to ensure you and your business stay protected.

"Every business is at risk of experiencing a cyber-attack and should be well-prepared to defend against these threats."

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.

Get your FREE copy today:
www.secureerpinc.com/cloudreport

Two-Factor WHAT??

Two-factor authentication (2FA for short), is a system in which you must verify your identity in two separate ways to access an account – this may be a login password, an online account or an account to access an application. Sound confusing? It's not. Here's an example:

After enabling 2FA on a Gmail account, each time you log in, you'll input your password. You then enter a six-digit code that is unique to you and changes every 30 seconds. You get this code from a smartphone app and input the code. Only then do you have access to your account. You must enter both password and 2FA code each time you access the account. If someone steals your password, they still can't access your account.

Two-Factor Authentication is <u>THE</u> best method to assure you are who you say you are.

If you aren't currently using 2FA with email and your most sensitive data and systems, ask for it. The extra 20 seconds to get logged in is short compared to the time spent dealing with a hacked account.- **R²**

Don't Come Back To Work

Don't come back to work. Instead, move forward in leading your company and managing your career by embracing remote work. Even though ghSMART has been remote-only for over 26 years, I never fully realized how enthusiastic I am about remote work until I heard that many companies are forcing workers to come back into offices.

Before the COVID-19 pandemic, "work where you want" was a rare concept – but during the pandemic, basically every company that could function with people working remotely shifted to that mode out of necessity. I thought that mode would stick, and we'd see the landscape of cities shift from "places people go to work every day" to "places people go to work sometimes, eat, shop, learn and play." But it seems I was wrong.

There isn't a great argument against the idea of remote work, but there is one *for* it. Remote work improves financial and operating performance and productivity for companies while also improving job and life satisfaction for employees. A 2015 Stanford University study published in the *Quarterly Journal of Economics* showed a 13% performance increase from remote working, and employee attrition rates fell by 50%.

Even with all of the research and information available that shows remote work is beneficial, there are still some myths floating around. For example, many say you can't build a great company culture when your business operates remotely. This is entirely false. I think an excellent culture begins with doing what's best for people. Making people commute to offices daily does not seem to be in anybody's best interests.

Another common myth states that people don't work as hard remotely as they do in an office. I believe that if you have a transparent culture where performance is measured, you can pay people according to the value they are creating. They will be incentivized to work productively and not lollygag – even if they are working remotely. But I guess many companies have not yet figured out how to pay employees based on a scorecard of measurable results and instead pay based on hours worked. They should be worried about lollygagging anyway, both in the office and for people who work remotely.

If you run or own a company, please continue to experiment with allowing your people to work remotely when possible. I believe this is the future of work, both because of the demonstrable benefits to companies in operating and financial performance and the benefits to workers due to having more control over their time.

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 *bestsellers. He stays active in his community and has advised many government officials.*

Working Remotely? Improve Your Work-Life Balance In 3 Steps

As many businesses continue to utilize remote workers, some employees are struggling to find a proper work-life balance. They constantly find themselves drawn back to their work after completing all tasks for the day, which takes away from their ability to enjoy hobbies or spend time with their families. Maintaining a proper work-life balance is beneficial to all aspects of our lives, including productivity and overall happiness. If you're struggling to maintain your work-life balance, here are three ways to include more personal time in your daily routine.

Set Boundaries: Don't allow yourself to be pulled back into work. Turn off your work phone and e-mail when your shift has ended for the day.

Create A Workspace: Do not work in the same areas you use for relaxation. This will make it more difficult to relax when you've finished working.

Dress Professionally: It might be tempting to wear sweatpants while working from home, but try to wear the same clothes you would wear if you had to go into an office. When the workday comes to a close, you can dress in more comfortable clothing, allowing you to easily unwind.

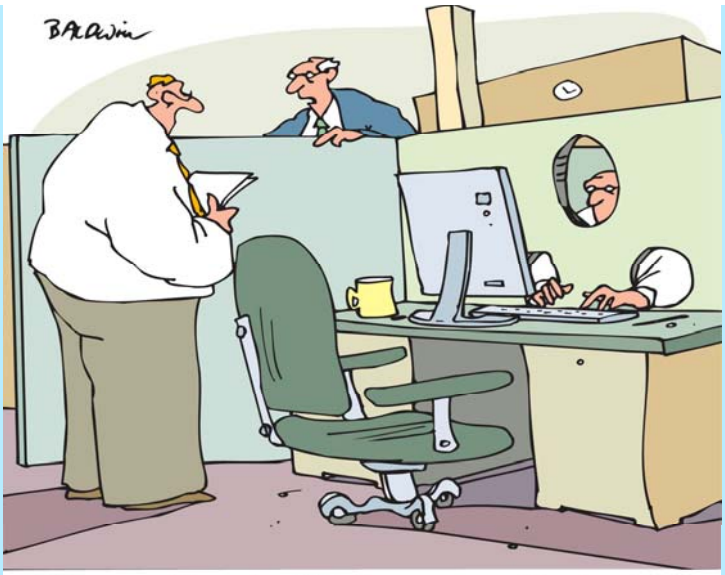
Is Your Workplace Becoming Toxic? Watch Out For These Warning Signs!

Over the past year, the idea of toxic workplaces has garnered quite a lot of attention. No employee wants to work in a toxic workplace and no business owner wants to run one, but how do you know if your business is gradually becoming more toxic? Here are a few warning signs to watch out for.

Mass Turnover: Are employees quitting in droves? Do you know why? You should be holding exit interviews with the employees who are leaving to determine why they want to work elsewhere. Allow them to speak openly, and you'll gain valuable insight.

Low Employee Morale: If your employees are not enthusiastic about their work or tend to work on individual tasks more often, you may have a morale problem. Hold a meeting with your team and allow them to speak freely to understand where the morale issue stems from.

Gossiping Employees: Are your employees talking negatively about each other or the business? If so, you must catch and correct it as soon as possible. Figure out why gossip has increased at your company and develop solutions to solve the root problem.



"According to IT, the security leak is coming from your workstation."