The Tech chronicle

March 2023

This monthly publication is published for family, customers and friends of

BRANDONBUSINESS machines

Our business is taking care of your business.

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 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.

Continued on pg.2

Continued from pg.1

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."

'I DIDN'T KNOW'

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

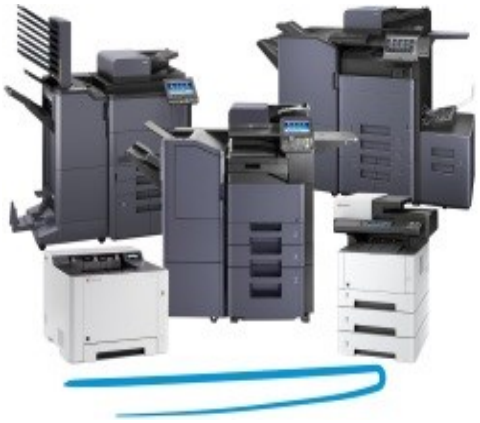
- That day a hacker steals critical data, rendering your office useless
- That day when your bank account or credit card is compromised
- Or that day when your customers' private lives are uprooted

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is this:

You Must Know How To Protect What's Yours!

Call us for a FREE Cybersecurity Assessment now!

Has your phone system let you down again?



If you have outgrown your current phone system or it is causing you down time or you're spending way too much on routine maintenance, we have the solution for your business. Thanks to our new Assurity Business VOIP Phone system, we can help you save a considerable amount of money AND give you more features and flexibility to support customers, and drive more sales.

Here are 3 reasons why our clients are getting rid of their current phone system:

1. **Drastically reduces your phone costs**
For most small businesses a premise-based phone system with its high upfront cost, hardware upgrades and maintenance fees is just not affordable. Eliminating the expense of a traditional phone system by moving to a modern VOIP system can save you up to 40%. Plus, if you have multiple offices or remote workers, our voice over IP technology integrates your data and voice networks to reduce long distance and lease line charges you are currently paying. We can provide your business with a lower-cost business class solution, allowing you to allocate those resources to other critical areas.

2. **Unparalleled Business Continuity**
Smooth communications are the lifeline of any organization. Without them, you interrupt business continuity. So, what happens in the event of a power outage or emergency? Unlike traditional phone systems that rely on power for connectivity, our hosted business phone services continue to operate even when other services are down. If weather makes traveling to the office difficult or dangerous, employees can leverage our system's capabilities at home to reroute calls and manage phone traffic. In a worst-case scenario of a fire, flood or other disaster at an office location, on-premise systems could be permanently damaged while a cloud communications solution continues to support you during the event and through your recovery. When planning a business

continuity strategy, companies should consider business class VOIP phone system as a critical component. While most businesses don't know costs related to defective phone services, the reality is that any unanswered call is potentially lost business that might never be recovered.

3. Improved Communications Help Build Your Business.
Assurity VOIP communication services enable the same sophisticated audio and video capabilities as even the largest players in the industry. A hosted solution allows access to modern applications like virtual auto attendant, unified communications, or products like voice, chat, data, and other technologies that integrate with your phone. Companies with Assurity VOIP communications improve customer service, employee productivity, and customer connections. Adopting the latest business communication applications transforms the way you do business and keeps your company on the cutting edge for a better collaborative experience with customers and employees.

Take advantage of these recent advances in phone system technology to move your business forward so you can save money, get better business continuity and improve your customer communications.

At Brandon Business Machines, we offer sales and services for the following:

- Multifunction Copiers
- Laser Printers
- Managed Print Services
- Document Management
- Managed IT Services
- Cyber Security
- Remote Back - Ups
- Disaster Recovery
- Wide Format Plotters
- Shredders and Folders
- VOIP Phone Systems

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.

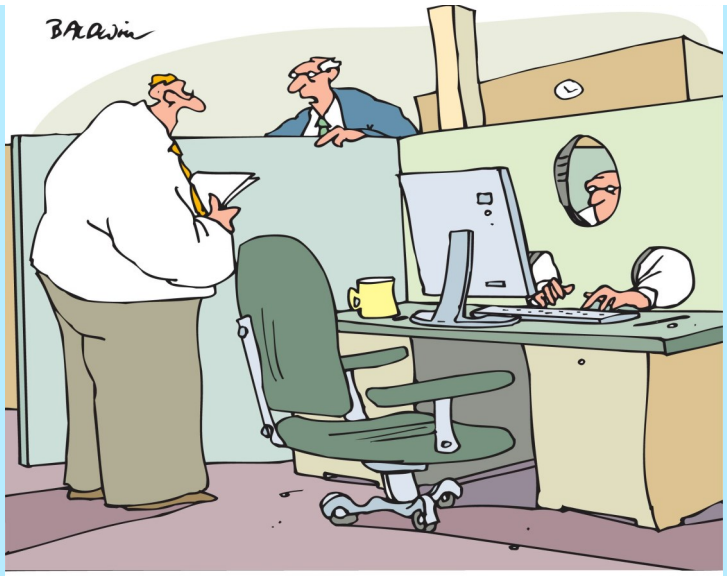
Is Your Workplace Becoming Toxic? Watch Out For These Warning Signs!

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."