December 2018

microTECH Times

Covered I.T. 24/7—Never Worry Again!

5 Tips To Keep A Cyber-Attack Away From Shattering Your Holiday Sprit

Is your data safe from a cyber-attack? Hackers love small businesses and more than half of small business will fall victim to a cyber-attack in the next six to eight months. Take a look at these five tips to protect your company this holiday season.

Why are small businesses a huge target?

Most business owners do not feel threatened; therefore their security is minimal - making it easy for cyber thieves to obtain vital information, such a personal details and trade secrets. To protect your data, you need to be proactive against a cyber-attacks. Consider the following:

1. Put a security plan in place. Cyber-security should be an automatic choice for all companies. However, more than 70% of small businesses do not have a formal security plan in place to counteract a cyber-attack. Some key elements of a good plan include: password protection, anti-virus programs, firewalls, software updates, and network monitoring. Big changes are happening every day; therefore, a good cyber security system should be as fluid as the environment. It should be monitored and updated on a regular basis to keep up with each and every threatening situation.

2. Layer your security efforts. Layering is important because even if an attack breaches the first layer of protection, the second and third layers may keep your data safe. Passwords should be the first layer of security and everyone should have their own login information and password. A strong password should be uncommon and consist of 8 to 12 characters that are combination of symbols and numbers, as well as capital and lower case letters. Other layers of protection include dual authentication, fingerprint, or even facial recognition.

3. Encrypt your data. Encrypted data is useless to a cyber thief without an encryption key. Many financial institutions have already integrated encryption into their data, and other business should follow suit.

4. Train your employees. For cyber security policies to be total effective, employees need to be trained and adopt consistent daily protocols. Cyber security awareness

(Continued on page 2)

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net

What's Inside

Holiday Giggles

Q: What do you call Santa's helpers?
A: Subordinate Clauses

Q: What do you get when you combine a Christmas tree with an iPad?
A: A PineApple.

Q: What do you call an elf who sings?
A: A wrapper

Q: How much did Santa pay for his sleigh?
A: Nothing, it was on the house.

Q: What type of car does an elf drive?
A: A Toy-ota

A Fresh Start; Happy New Year!

Wrapping up the end of the year is always a challenge, but well worth it. We get to see the accomplishments of the entire year and make fresh goals for the new year.

Happy New Year!

New years is time for a fresh start. Many people make resolutions to help them focus on a better path in life. We encourage you to do the same for your business. Resolutions for better security, network stability, or even an equipment refresh can help you push your organization to the next level.

It all starts with one initiative. Feeling overwhelmed by the array of choices for your focus? Tired of slow computers? Feel like your data is held hostage loading 1/2 the time when you need access to it? Sit down with the leaders of your company and review the greatest pain points from 2018. Develop a new resolution for your business to evolve beyond the delays. Out pace your competition with new initiatives to

(Continued on page 3)

5 Tips To Keep A Cyber-Attack Away...

(Continued from page 1)
requires ongoing training. Employees need to be reminded through refresher classes and updated security tips to keep policies in practice to ensure your company is safe.

5. Back-up often and check them regularly. Cyber-attacks happen in a variety of ways. For instance, a hacker could lock you out of your operating system and release it only in exchange for ransom money. When you have a systematic back-up in place, data could be restored and the hacker could be left holding an empty bag.

The bottom line is to always be on the defense. It has been said that the best offense is a good defense. Remember, no organization is safe from a cyber-attack. When trade secrets and customers' personal information are obtained by hackers, it can be a total train wreck. Disruption in normal business operations falls to the bottom of the list because you will lose much more than time. You can lose the confidence of the general public, money, and future business due to outraged customers who may publically speak harshly about your company and its practices.

Hackers just need a small gap in security to make a big negative impact, so any investment you make to prevent a cyber security breach is money well spent. So, give your company the upper hand. Give us a call today for your Network Security Audit and you will receive a full evaluation of your current environment as well as recommendations to be proactive about your security.

Micro Enterprises LLC 877-540 -6789

A Resolution For Security: Facebook Firewall

Internet access provided to employees for business purposes is a necessity, but also leaves your company information and the entire network vulnerable to security risks.

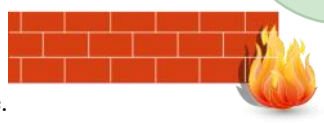
Is productivity suffering because of social media? Productivity severely suffers when employees engage in social activities online such as logging into Facebook several times a day, constantly making personal phone calls, and participating in office gossip. Even seemingly small posts on a social media site about the declining profits of the organization can damage your organizations reputation. You may be surprised how many eyes will see this confidential company information. Don't let any form of social media affect productivity or impact your business. Employers have the right to change or update policies at any time.

Reduce this risk by blocking certain sites. Many companies block certain sites that are known to be catalysts for computer malware distribution or have been deemed inappropriate for the workplace. Twitter and Facebook make the list of commonly blocked sites by over 50% of U.S. companies.

Social networking style sites are more susceptible to cyber-attack. For instance, Facebook was hit with what was deemed the "Koobface" virus". This virus sent messages supposedly from your friends, but these messages, once opened, were linked to a virus which could ultimately infect your entire system and expose your private information to the world.

Firewall configurations specific for social media will save resources. Employees can be restricted from watching videos, playing games, or browsing the internet for non-work related activities directly through your firewall. Take advantage of this powerful tool you may already own, and configure it to safeguard your business.

Outdated firewalls are just like coal in your stocking. Technology is evolving at lightening speeds and outdated firewalls are just useless. Keep your firewall properly maintained with active licensing. Consult your IT guru regarding Internet security. Implement security strategies that will keep your confidential data safe.



Gadget Gifts

Yeah, we all love this time of year. There is nothing like a new gadget to brighten the season.

Audio fun. The Jabra Elite 65t is a fantastic way to treat your special someone to an earful of wireless fun. This sleek new in-ear headphone set offers comfort and exceptional audio quality.

Fun on the go! The new GoPro HERO7 is an action camera that's ready for any type of activity. It can capture 4k video at 60 frames per second. The eye catching quality coupled with the best stabilization tech in its class, ensures all your adventures will be captured with impressive detail.

Echo with a kick. If you've experienced the Amazon Echo, the all new Echo Plus (2nd Generation) Smart Speaker is truly a treat. This new Echo is Dolby-tuned and delivers 360 sound with the most robust base we've seen yet.

Communication toys. The new iPhone X and Samsung Galaxy Note9 smartphones offer a plethora of new features and advancements. The displays are beautiful and the cutting-edge hardware inside is sure to please anyone on your list.

A Fresh Start...

(Continued from page 1)
grow your company and develop a strategy from the inside out.

Don't just make do; get a new one. Sometimes, it's not about fixing things that are broken; it's about putting better tools in place for your staff to be more productive. A resolution to refresh your network tools may be the best way to boost productivity and enhance your business.

A proactive resolution. Stay on top of the day-to-day activities in your company, good and bad, so you can develop a list of meaningful initiatives. Make a list of things that will help you meet your goals throughout the year and take a proactive stance for your future. Think about the next steps to make those dreams a reality and build a plan. Taking the first step always seems to be the most difficult, but you may find that your staff really wants to see the company grow as well.

Communication. Keep everyone in your organization informed of the upcoming changes. You may even want to send a letter or message to your clients so they see your growth and progress. Let us know if we can help with any of your new resolutions.

Be Prepared For Unexpected Power Outages

Are you prepared for the next big unexpected power outage? Power is necessary to run your business, but what happens when the power suddenly goes out? Your company could lose a ton of money. Having a plan in place will reduce downtime.

What constitutes as a power outage? Short or long time periods of power loss in a particular area is considered a power outage. This can affect your home, business, and even entire cities.

There are three types of outages. Brownouts are when the voltage decreases and lights dim. This type of outage could cause electronic equipment to malfunction and fail. A blackout is a power loss to an entire area. This type of outage could last a few minutes to several days/weeks. A permanent fault outage refers to power loss due to power line failure. It doesn't matter the type of outage you're dealing with, always be prepared. As reported by "Inside Energy", the annual average of power outages has doubled in the United States.

How can power outages affect your business? Your business could be affected in a number of ways. Here are just a few:

1. ***Loss of business.*** Many businesses experience a loss of customers and/or income due to the inability to operate normally during a power outage.

2. Employee productivity takes a dive as they are unable to complete their work due to equipment failure which often leaves paid workers sitting stagnant.

3. Data loss. Computers are complex and they need to be shut down properly. Power outages cause computers to shut down abruptly and open files could be lost. This can also cause hard drive errors or even failure.

Equipment can be totally damaged during a big power outage. Replacing equipment before its time, due to unexpected power surges, is a large unexpected cost many business owners do not even consider.

How to minimize the negative effects of a power outage. Power outages can occur at any time and bring your operation to a screaming halt. Be prepared with these quick tips to avoid major losses:

- Have a plan to deliver services and products to your customers whether you have power or not.
- Educate all your staff members and practice emergency response drills.
- Invest in uninterrupted power supply units, better known as UPS devices. They will ensure your equipment is shut down property and in effect minimize hardware damages and prevent data loss.
- A back-up generator is a simple way to minimize unexpected computer downtime. A trained professional can help determine the proper generator size for your business, install it and recommend regular maintenance routines to keep it working in case of an emergency.

Know your needs. Power outage, flood, or fire, know what you need to keep your business going. An ounce of prevention can save you a ton of money.

"We make all of your computer problems go away without adding additional full-time I.T. staff!"

Ask about our fixed price service agreements — Computer support at a flat monthly fee you can budget for, just like payroll!

Inquiring Minds...

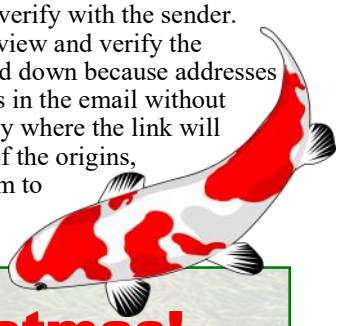
3 Most Notable Phishing Attacks Of 2018 And How To Avoid Them. This year has been a whole new stream of phishing scams. From MailChimp to the IRS, is there nothing safe these days? No, not really. We must all stay informed of trending phishing scams to avoid disaster.

Malicious e-mails sent from MailChimp. In the first quarter, MailChimp experienced a security breach in which many accounts were compromised. Attackers were quick to abuse the open accounts and send phishing campaigns to the e-mails listed. They arrived with .ZIP archives which concealed a terrible infection dubbed GootKit infostealer. Later investigation revealed that the compromised accounts were actually breached because of weak passwords or reused credentials. Just goes to show, unique user names and strong passwords can help keep your information safe online.

Accounting association spoofs. By the second quarter of 2018, crafty criminals were focused on tax professionals. A series of fake emails were sent to tax offices across the nation requesting verification for their logins to the tax professionals' accounts. These logins literally handed the attackers their clients' data. This information was later used to process fraudulent tax returns or was sold to the highest bidder.

O365 even has a few nasty scammers tagging along. Later in the year, Office 365 users reported a phishing email with the subject line of "Rules of Conduct." The message is positioned to appear from the company's HR department and asks the recipients to review a PDF with the company's rules of conduct. Of course, we all want to stay in HR's good graces so those who clicked on it are then led to an excel file and are redirected to a website to log into their account online. Once the credentials are entered, the hackers have what they want and can see all your email, copy your information and even send messages too.

Quick tips to avoid phishing scams. If you are unsure at all, about an e-mail, pick up the phone and verify with the sender. If there is no number to call, be sure to view and verify the sender's address but don't let your guard down because addresses can be spoofed too. Never click on links in the email without hovering over the link first to see exactly where the link will take you. If you aren't absolutely sure of the origins, you can use a website like virustotal.com to check the URL against a database of known scams.



Merry Christmas!

It's time to close out 2018. New acquaintances and legacy clients, we'd like to take a moment to say thank you so very much for your continued support and business. You are instrumental in our success and we are honored to serve your organization. It has been a bountiful year filled with new connections, office moves, add-on employees, equipment refreshes and even a few emergency situations. Ok, maybe I'm embellishing a bit there—quite a few emergency situations. However, we are proud to say we have worked through each hurdle, thick or thin, with our clients to find solutions that foster stability and growth. But, we couldn't do it without you. So…

Thank you for including us in your operations!

From all of us, to all of you, we wish you and yours the most wonderful Christmas and a very Happy New Year!

microenterprises

PO Box 503
Deepwater, NJ 08023
877-540-6789
www.microent.net