Happy Halloween!

October 2018

microTECH Times

Covered I.T. 24/7—Never Worry Again!

6 Tips To Keep Creepy Little Hellions From Haunting Your Network And Secure Your Company Data

Businesses of all sizes are greatly reliant on information technology these days for a variety of operations. From bookkeeping and account documentation to communications and industry specific software, companies use technology to keep their daily operations rolling.

Technology at your fingertips. Availability is a top priority for all our clients. They just want everything to work and be available when they need it most. A broken computer, network that moves as slow as molasses, or an infection can create a very sticky situation stalling your business. Ultimately, time is money and the more time you spend chasing down pesky IT problems, the more potential revenue floats out the door.

Band-Aid solutions leave open wounds for creepy little hellions to wiggle their way in. Often times, businesses come to us when they've tried everything to Band-Aid recurring issues. They are truly looking for a more comprehensive solution. They have seen how the quick fixes and sloppy security measures don't last and leave openings for attacks. Here are six tips to help you keep creepy little hellions from sneaking into your network.

1. Run a services audit on your equipment. Make sure everyone on your network is supposed to be there and every workstation is up-to-date with vendor patches and updates. In addition to shoring up security on the each device, these audits may reveal additional services running on your servers that are unnecessary or open ports that make the entire network more vulnerable. Fortunately, it is pretty simple to take care of these concerns. However, ongoing review and upkeep are essential to ensure continued security.

2. Update your firewall and router too. These two devices are

(Continued on page 2)

What's Inside

Spooky Quotes

"It's Halloween, everyone's entitled to one good scare."
~ Brackett, Halloween (1978)

"I've seen enough horror movies to know that any weirdo wearing a mask is never friendly."
~ Elizabeth, Friday the 13th Part VI (1986)

"Be afraid… Be very afraid."
~ Ronnie, The Fly (1986)

"Oh look, another glorious morning. Makes me sick!"
~ Winifred Sanderson, Hocus Pocus (1993)

Flip Your Witch Switch

Go ahead and flip your witch switch. It's Halloween at the end of the month, dig in deep and find your inner child. Enjoy this fun filled holiday with family and friends.

Dress up. Witches, pirates, and things that go bump in the night are all time favorites for Halloween costumes. To be cool, check online to scope out new trends for 2018. This year we're bound to find a handful of Black Panther, Wonder Woman, and other super hero costumes with the recent move releases. Take some time to order ahead of time so you have your best threads for this fun occasion.

Saturate yourself in the season. No, you don't have to down a pound of candy to enjoy Halloween. There are plenty of healthy options on Pinterest to help you infuse a variety of fruit and vegetable treats into your spread.

Decorating and décor. Over $9 billion is spent annually on decorations, candy and cos-

(Continued on page 3)

microenterprises

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

What Is A NAS?

A NAS is a Network Attached Storage device that can store and share data for multiple computers.

Physically, a NAS is like having a private cloud in your office that is fast and inexpensive. This type of devices is generally used as a part of a data backup solution.

What does it do?
A NAS system offers space to store copies of data from your networked devices. This data is continually accessible making it simple to recover files and collaborate.

Who needs a NAS? Small to mid-sized companies often use a NAS device as one component of their backup solution. This onsite piece of equipment may be the first piece to your backup and disaster recover plan. However, we recommend a second off-site backup just in case your office is physically compromised by thieves or natural disasters.

6 Tips To Keep Creepy Little Hellions...

(Continued from page 1)
often overlooked since they are generally put in place and not seen or touched day-to-day. However, routers and firewalls should be updated at least annually to ensure the most recent licensing, security updates, and bug fixes have been applied.

3. Disable file sharing on your work computers. With the exception of your file servers, there really should be no reason to use file sharing services on your laptop or computers. Leaving these services active allows anyone using the same public Wi-Fi network to see all the files located on your device. Disabling this feature will help secure your computer from prying eyes.

4. Use private IP addresses.
If you have a business that uses a Dynamic Host Configuration Protocol (DHCP), consider locking down your IP addresses. Instead of sitting back and allowing your router to assign IP addresses to devices on your network, lock down the addresses so you can clearly identify suspicious activity in your router logs and smoke out inconsistencies.

5. Implement and maintain antivirus on all your devices. Antivirus protection or AV, helps prevent, detect and remove infections before they take over your network.

6. Control IT costs. Some business owners think of their equipment as a one-time investment. They buy a handful of computers, a server, a firewall and the software they need to get their business started, then their ready to party! Right? Nope. I wish it was that easy. Technology is not a one-time investment you carve into your business. Overtime your company will require new computers, software upgrades, new tools and even a new server. Don't wait until things break to develop a plan to replace your equipment or upgrade your software.

Need help? Give us a call. We offer a Network Security Assessment to map out your infrastructure, help you identify vulnerabilities, and learn how to further safeguard your business.

Micro Enterprises LLC
877-540 -6789

Hackers Are Bobbing For Apple Macs

Historically, Apples Macs have rarely been a target for hackers. However, these past few years have been trying for Apple lovers. Attackers seem to be more focused on exploiting weaknesses believed to affect all Apple Mac equipment.

Apple Macs are just safer, right?
We always hear people say they want Apple products because they are safer to use. While it is true, in the past Apple Macs were rarely a target for hackers, a new age of attacks is brewing and Apple users should be very cautious.

WindTale and WindTape take flight. According to Karim, a researcher at DarkMatter (a reputable cybersecurity company), attackers have now found a way to get around all the native macOS security measures. WindTale and WindTape are just a few examples of malware that were specifically engineered to dig into Apple products, screen shot user activities and infiltrate files on the computer.

How do these attacks happen?
Apple Mac products are still largely protected from harm. Phishing e-mails seem to be the largest culprit for infections. Here's how it happens:

1) User receives a spear phishing e-mail containing a link to a site
2) A .zip file containing the malware is downloaded automagically when the link is clicked
3) The malware seeps into the macOS

It's as easy as bobbing for apples.
Clever hackers send loads of these e-mails daily to bob for unsuspecting Apple users. Be aware of the dangers. Do not open e-mails from people you do not know. Always double check the e-mail address do not click on links in e-mails if you are at all concerned. Go directly to the vendor website or call the company to ensure the message is legitimate.

Unforeseen Catastrophes

Going into business is heavy with financial risk but, once in business, natural disasters or unforeseen problems can create catastrophe.

Fire ranks high as a potentially devastating risk for business. More than 75% of companies that experience a serious fire go out of business within three years of reopening, according to Phoenix Fire Protection.

Proper insurance can cushion the destruction of assets and business interruption costs, but it won't help the loss of customers, employees, or data.

Data loss may be the easiest to mitigate of these three risks. Daily off-site backups are key. On-site backups may seem sufficient unless a fire begins on the weekend or a holiday. Be sure to check backups regularly and assign at least two people who know how to retrieve backups.

Plan for disasters.
Here are a few critical questions to get you started: How can you protect IT equipment from fire or other disasters? How will you retrieve data? Where will you operate? Take an inventory of all your assets including your IT equipment and develop a plan to rebuild your business.

Flip Your Witch...

(Continued from page 1)
tumes. So, set aside some time to decorate. Pumpkin carving has truly become an art. Creative folks carve everything imaginable into pumpkins from animals and cartoon characters to famous movie stars and seasonal scenes.

Trick-or-treating, is a time honored tradition for most families this time of year. I still remember when I was a kid, my father dressed up with a gas mask, a crazy grey haired wig, and navy blue automotive jump suit following my friends and I up to each house. He would stand idol in the street, scaring all the other kids as they walked by.

Halloween safety tips. While trick-or-treating is fun, roughly 180 million Americans will be celebrating this Halloween and it's important to stay safe. Always accompany young children when they are ready to hit the streets for treats. Bring flashlights with you to avoid mishaps on stairs and unsteady porches. If you are driving, keep your eyes open for scared animals racing across roads and children walking in dark because costumes may make their presence more difficult to detect.

3 Frightening Online Scams To Watch For

With technology, evolving fraudsters have turned to the Internet to commit their crimes. Scams Online are becoming increasingly popular and many people are falling victim to them. Here are just a few of the most common scams online to look out for and avoid. Share these with your coworkers and friends.

1. Travel fraud. A travel agent or company you have never spoken to before, offering a vacation or travel accommodations at a very low price, contacts you unexpectedly via e-mail or phone. Even though you've been meaning to plan a get away or work is calling you out of state soon, this may be a costly mistake.

Signs to spot these crafty scammers. Often, people are asked to pay via bank transfer. Always be certain of the company you're speaking with. Ask for a phone number to call back and call it. Look closely at the details, pictures or address of the property or hotel included in the offer. If anything seems suspicious, be very cautious.

Protect yourself. First do not reply to the e-mail or click on any links or attachments within the e-mail. These may lead to malicious websites or even download a virus. Then report the suspicious e-mail to your e-mail provider as phishing.

2. Online auction and seller fraud. So, you're overhauling your network or office space and want to find the best deals? Watch out for online auction sites and sellers that claim to have the best prices on computers and furniture but really are out to get your money.

Signs to spot auction and seller attacks. Review the sellers account online. Do they have bad feedback in their history? Google the information you have about the seller, name, alias, phone number to see if there is anything negative posted about them online.

Protect yourself. Pay on the auction site every time and do not click on links the seller sends to you directly. Never pay by bank transfers, instead use a recognized service such as PayPal which offers a payment protection policy.

3. Social engineering scams will take you for a wild ride. You have been in and out of the office all day and you receive an urgent e-mail message from your boss; he would like you to run out to the store and buy some iTunes gift cards. Sure, he's asking, it's his money, he's in meetings and you've got a little time before your next meeting. However, this does seem strange.

Signs to spot a social engineering scams. Social engineering is constructed using data familiar to you to trick you into believing they are a trusted resource. The ideal is to psychologically manipulate you to perform actions and divulge confidential information.

Protect yourself. Check who the actual e-mail is from. Is the e-mail exactly what you see when your boss really sends you messages? If you notice any change, no matter how slight, to the e-mail address or misspellings in the message itself just pick up the phone or talk directly to your boss to verify the message. Don't buy anything until you know for sure what the request is all about.

Worried about scammers? Inform your staff of these online scams and how to protect your company from fraud.

"It's a conflict between your hardware and your software. Your cauldron won't support Eye Of Newt 3.0."

"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...

The Growing Market For The Internet Of Things Poses Increased Security Risks For Businesses.

More electronic devices will soon connect to the Internet, providing more convenience and information, but this Internet of things also brings new security risks for businesses, according to security provider Malwarebytes. Privacy issues top the list of concerns. Devices that include always-on cameras, auto-answer features, and microphones are prime targets for hacking by criminals hoping to steal, infect, or just harass consumers.

Those with smart appliances essentially agree to data collection and sharing when they make their purchases. Some smart refrigerators, for instance, keep track of what kinds of food you buy and can be integrated into applications to purchase groceries online. Televisions can keep track of what you are watching, and AI-powered devices like Alexa and Google Home keep a record of your search history. Depending on the fine print, that data can then be used to send you targeted ads or be sold to big data analysis companies. These always-on devices often leave openings into your internal network as well since they are connected to the Internet.

Vulnerabilities can and will arise that allow hackers to take control. Cars with automatic driving capability, for instance, opens the door for tech-savvy criminals to take over and ransom the vehicle back to the owner or even cause a crash. Recently, it was discovered that multifunction printers can allow hackers to deposit malicious code into a business network. Security for these seemingly innocuous items is essential to ensure your entire network is safe from attacks.

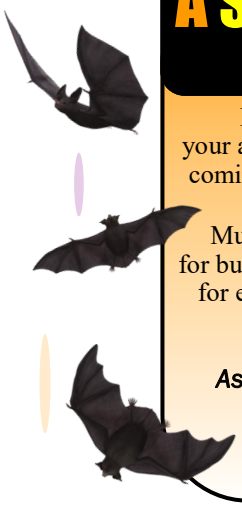
Internet-enabled devices like security cameras may also act as a backdoor. Even large companies like Twitter, Netflix, and CNN have had to recently address vulnerabilities with security cameras. Remember there is usually very little protection built into these seemingly harmless connected devices. Instead, device safety depends on the security of the network, where strong passwords and additional protocols are essential.

Before you buy an Internet connected device, make sure it doesn't have a generic username and password. If it does, set a strong password and be sure to update it quarterly. Keep in mind, standard manufacturer passwords are posted online by manufacturers for consumer ease of use. However, this also leaves an open invitation to hackers.

Ready to install a new router, printer or security camera system for your business? Give us a call. We recommend a full Network Security Audit after your new equipment is installed to ensure there are no open areas for hackers to exploit.

microenterprises

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



A Sweet Solution For A Very Scary Situation

It's Monday, you sink into your desk chair and all the sudden your all-in-one fax machine seems to rise from the dead. There is no fax coming in but, it sure seems to be busy over there. You're the only one in the office, so is the darn thing just possessed?

Multifunction printers and all-in-one fax machine are a known risk for businesses. These devices may be connected directly to your network for ease of use but, left unsecured leaving a back door open right into your network where attackers can wiggle in malware.

Give us a call today for your ***Network Security Assessment*** *and we will review every device connected to your general network to button up security loopholes.*

Micro Enterprises LLC • (877) 540-6789