April 2019

Happy Earth Day!

microTECH Times

Covered I.T. 24/7—Never Worry Again!

5 Top Cybersecurity Threats In 2019 Unearthed And How You Can Secure Your Company

Data breaches, hacking, and skimming -- all of it poses a threat to consumers and businesses during 2019. Be aware of these top 5 threats that are on the rise this year and learn how to secure your company.

"Today's hackers are very deft at outsmarting security measures," said Michael Bruemmer, Experian Vice President of Data Breach Resolution, adding that, "cybercriminals always seem to stay a step ahead of new security gates." According to the Identity Theft Resource Center (ITRC), data breaches increased sharply in 2018 with 1,027 breaches reported and 57,667,911 records compromised.

Experian's 5 top threats for 2019 are really a bit of a shock. Biometric hacking, skimming major financial institutions, attacks on wireless carriers, breaches on cloud services are just a few listed. Take a look at the top five and learn how to protect yourself and your organization.

1) Biometric hacking and detecting flaws in touch ID sensors, passcodes, and facial recognition are a new wave of attacks. Although biometric data is still the most secure method of authentication, it can be stolen or altered. So, don't get to comfortable with the new features released on cell phones and laptops. Lock down your business and personal accounts with Two-Factor Authentication (2FA) whenever possible.

2) Clever skimming techniques on major financial institution's accomplished with hidden devices to steal credit card information, and invade bank network computers with undetectable malware are on the rise. Protect your accounts online with 2FA, use a password manager even on your cell phone and

(Continued on page 2)

Earth Day Celebrations

April 22nd, 2019 is Earth Day. The Earth Day Network's theme this year is protecting our species from extinction. Take a look at how Earth Day became a national observance and what you can do to join the fun.

The "Father of Earth Day" was U.S. Senator Gaylord Nelson. He began promoting environmental activities in 1962 and eventually convinced President John F. Kennedy to tour the nation in support of environmental concerns. Even though his initial efforts didn't catch on, in 1970 he proposed a National Earth day. He planned a nationwide environmental protest with the hope to get everyone involved and he sure did.

20 million Americans supported the protest on April 22nd, 1970. This first Earth Day celebration had an amazing impact raising awareness about the limited resources on our planet and how the things we put in the air, water, and earth are truly impacting the

(Continued on page 3)

Global Insight

Did you know:

- Almost half the weight of the earth's crust is accounted for by oxygen.
- The Amazon rainforest produces more than 20% of the world's oxygen supply.
- About 27 tons of dust rains down on the earth each day from space.
- Of all known forms of animal life ever to inhabit the Earth, only about 10% still exist today.

The Dirt

microenterprises

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

5 Top Cybersecurity Threats...

(Continued from page 1)
always, verify e-mails from your banking institution by logging directly in to your account online to view messages or information.

3) Attacks on significant wireless carriers have simultaneous effects on iPhones and Androids, stealing personal information from millions of phones and possibly disabling wireless communications. This type of target is virtually impossible to prevent from a consumer level however, how you use your devices could be a saving grace. Do not keep critical business or sensitive personal information on your cell phone. These files can be compromised if your carrier is attacked.

4) Cloud provider vulnerabilities. A breach in the security operations of your cloud vendor could jeopardize your sensitive information too. Not all cloud services have proper security in place. Be sure to ask questions when implementing a cloud solution. Is your data encrypted when it is not being used? Is there strong physical security at the datacenter where the cloud is hosted? Is there a firewall solution? Are their intrusion detection systems with event logs and someone monitoring them? Be aware of the risks and how to protect your company data.

5) The gaming community will be faced with cybercriminals posing as gamers for access to its computers and the personal data of trusting players. According to the ITRC, significant breaches from 2005-2017 rose from about 200 per year to more than 1,300. Billions of data pieces have been exposed, allowing cybercriminals to monetize stolen data, leading to an increased risk of identity theft. While this doesn't seem like an issue that would impact your office, many workers use their laptops for personal gaming when they are away from the office. Put the proper security in place to avoid a breach by implementing an Acceptable Use Policy so everyone knows what is expected.

Where do I start? Create and implement a Bring Your Own Device (BYOD) policy and an Acceptable Use Policy to set the standards for your staff as well as reduce the risks for an attack. In addition, implement 2FA wherever possible to lock down your company applications and information.

Need help? Give us a call today. We will conduct a full review of your network and security to ensure you have all the latest updates and preventative measures in place.

Micro Enterprises LLC
877-540 -6789

The Scoop On Why Every Small Business Needs IT

In today's world, everything is digital. It's important that your business has the tools to keep up. Even if you are a business that isn't in tech you need an IT person to make sure that you are staying on top of things and to keep things running smoothly.

Why is IT so important? One of the key reasons why IT is so important is because your customers depend on you to make sure that things are easier for them and that their information is secure. When trying to interact with your customers they always depend on what's the most convenient for them. In order to do that, you need the technology to digitize everything you can including inventory management, scheduling appointments, HR functions, and accounting as well as keep it secure.

Your customers are placing their business in your hands and they want to know that their information is kept safe. They chose to work with you and expect their business with you will be taken seriously. An IT provider gives you the confidence to tell your customers, their information is safe with you because of your proactive approach.

An IT team can make sure that you are capable of providing all of the things your customers truly need. If you do things to make your customers happy, ensure their security, and make it easier for them to work with you they are going to keep coming back for more. So, while you may see IT as an unwanted expense, also recognize that it will actually bring you more profits in the long run.

Small Business Survival

Did you know that only about half of small businesses really survive? What is the secret to success? Longevity? Making money?

Establish a brand and treat your staff with care. Build a brand that everyone can be proud to stand behind and focus on supporting your staff in their personal lives so they want to be good Stewarts for your organization. Provide benefits and perks to keep them engaged with your company mission.

Manage money and be ready to scale. Every business has it's own road map to success, but two things are sure to impact daily operations, how money is managed and how the company grows. Don't stunt your business with poor planning. Outline your three and five year goals for growth before you invest in resources for your company.

Offer quality tools. You've got a good brand, business is flowing, your staff is proud, you're poised for growth, now it's time to focus on your tools. Take time to evaluate your infrastructure. Ask your staff for feedback and take note of ongoing operations challenges. Invest in tools that are affordable and scalable.

Earth Day...

(Continued from page 1)
world. Today, Earth Day has become a Global event with over 180 countries and more than 1 billion people supporting the cause each year.

Protect species from extinction. This year, the Earth Day theme is all about protecting species from extinction. Studies estimate that we are losing species at an alarming rate, far higher than normal. Some species are even disappearing before we have a chance to really study them. So, the campaigns you will see are focused on raising awareness about the accelerating rate of extinction and the consequences of this phenomenon.

What can I do?
There are a handful of ways to get involved and no, you don't need to protest in the streets with huge signs. Visit: www.earthday.org to learn more about the Earth Day Network, partnership opportunities, campaigns, or even make donations. Earth Day is all about learning how small collaborative efforts for environmental change can make a big difference. Join the mission to broaden and diversify the environmental moment world wide and build a healthier more sustainable Earth for future generations.

How Does Two-Factor Authentication Actually Work?

A variety of applications and accounts online now offer password protection with Two-Factor Authentication (2FA) too. This security combination will help you keep all of your accounts locked down. Take a look at these great password tips and learn how 2FA actually works.

Password tips. When creating passwords it is important to create a strong one. Many hackers do not have the tools to figure out stronger passwords. You need to make sure that your password is unique. The best way to do this is to use random strings of letters, numbers and special characters, do not use real words. Creating passwords with those unique tools makes it very tough for anyone to figure out.

Shake things up. You should also never, ever use the same password twice. It is always easier to remember one password as opposed to having to remember a different one for every account, but sometimes it's worth the extra effort if you have secure data that you do not want a hacker to get into. If you have a tough time remembering passwords, sign up for a password site such as LastPass, they help you save your passwords all in one secure location. Password programs like LastPass even offer business plans so you can share accounts with other authorized users safely.

Why aren't strong passwords enough? Login's were created to restrict the use of an account or program only to the preapproved user logging in. Unfortunately, malicious criminals attack everything these days from government entities, to companies and even personal accounts online. Changing your password regularly can help deter an attack but may never eliminate you as a target. In addition, we are all human and have lousy memories and a ton of login credentials to remember. At some point security fatigue sets in and you find yourself using one password for everything again even though there are really no signs that cybercrime is slowing down.

Take every precaution to protect yourself and your company.
Two-Factor Authentication is an additional layer of security. If you have a program or site that offers a 2FA feature you should take advantage of it. This makes it impossible for hackers to get into your account.

How does 2FA actually work?
Not only do you use your strong password to log in, but you also need another verification method such as a text message authorization, e-mail confirmation or authenticator program code to open your account. This is how it works:

- Go to your site and log in with your user name and password
- The 2FA pops up on your screen asking for your authorization code
- You check your text, e-mail or authenticator app and enter the code displayed
- After the code is verified, the account is logged in and ready for use.

Get started today! Need help implementing a company wide password management system? Want to learn more about 2FA? Give us a call, we're here to help.

"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...

Why Are Software Updates So Important? If you have outdated software you are putting your business data at risk. Not upgrading your software can leave your system open to hackers. It can be frustrating having to update things on a regular basis or having a pop-up notification when you are in the middle of a task telling you that it's time for an update. However, if you keep putting off those updates and never do them, then your computer and your important business information will be at risk.

If your software is behind, that can lead to frequent and lengthy IT outages. If you're constantly having to call for IT help then you're losing money and important time. The best thing to do is set up a time to do the updates on a regular basis. You can pick a time each day to be sure that your system doesn't need to be updated. Technology is constantly growing and changing. It is designed to grow with everything around it that is constantly evolving too. If you get far behind, data can be lost with newer versions of the technology and you may end of leaving your company vulnerable to an attack.

Software upgrades are not something to ignore. It's important if you value your companies security, profitability, and productivity to keep all your systems updated. Be sure to set up the tools that you need and reminders to keep your business software up to date and continuously check to see if you have the latest technology for your business needs. Don't forget your servers, firewalls, laptops and mobile devices fall into this same category. They all require regular attention to stay current.

Phishing Attack Tips; Don't Take The Bait! There have been a lot of phishing attacks and un-wanted e-mails with attachments lately. Here are some great security tips to share with your staff so everyone can stay on top of e-mail attachment security.

1) Do you need it? If the e-mail has an attachment, before you open it, make sure you **need** to open it. If you don't **need** to open it, then don't open it.

2) Do you know what it is? If the e-mail has an attachment, and **you don't know** what the attachment is for, don't open it!

3) Do you know the sender? If the e-mail has **unsolicited** information about some expiring accounts, past due invoices, unclaimed money, bitcoin investments, C1al$is and Vi@gra medication, or other Nigerian prince related nonsense be weary.

As a general rule, unless you specifically requested that someone e-mail you a file or you're unsure who sent you the message, don't open the attachment. Attempt to reach the sender by phone to confirm the file.

microenterprises

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

Claim Your Network Security Audit Today!

Running your business is complex enough without technical support and cybersecurity concerns. Everything rides on one thing, the reliability of your network. ***Do you know if your computers are up-to-date?*** Does your firewall have the latest licensing? **Are your e-mail accounts secure?**

Give us a call today for your *Network Security Audit* and unearth a full report of recommendations for your network and learn how to keep your company safe.

Micro Enterprises LLC 877-540 -6789