wyant computer services

TECHNOLOGY TIMES

"Bringing you opportunities and proven solutions to your technology challenges."

February 2020

If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or the business does have some security but it isn't set up correctly.

At the same time, cybercriminals send e-mails to businesses (and all the employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give the criminals the information they want. All it takes is ONE employee to make the click.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the capability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the ransom only for the cybercriminal to delete all of their data anyway.

Continued on pg. 2

Check it Before you Share it!

It is impossible to escape hearing about FAKE NEWS. Even those of us who know better can be guilty of spreading false info. Just last week I shared a FaceBook post that was garbage, luckily I have very good friends who pointed out my error and I deleted it right away.
Here are a few quick ways to avoid promoting false information.

- Stop! Don't hit that share button. Take a few extra seconds to check your information.
- Google Search: Cut & Paste it into the search bar; see if other reputable sites are reporting on it.
- Snopes.com: is one the best fact-checking website on the internet and has been around for a long time.
- Hoaxy: this search engine was built by Indiana University and the Center for Complex Networks and Systems Research, it tracks and integrates social sharing of links published by trusted independent fact-checking organizations.
- Check the URL: if it looks suspicious it probably is, watch for the misspelling of words. If the website does not have much content like a Mission Statement or list of members, board or employees you should not trust it.

Cut & Paste is your friend: check that quote, article or picture make sure that someone hasn't made changes to it fit whatever they are trying to spin. Here is a great article for more information: https://www.lifewire.com/spot-fake-news-sites-4122407. by Wendy Roberts

This monthly publication provided courtesy of Tom Wyant, President of Wyant Computer Services.

Need Information About Our Services Go To: https://www.gowyant.com/

Continued from Pg. 1

The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you.

Cybercriminals can do more than just major damage to small businesses; their actions can literally destroy a business! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners fall into the habit of complacency. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of vulnerability.

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, which will put your business and customers at risk. Or you can take it seriously and put IT security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

7 Things TO DO So You DON'T Get Hacked When Shopping Online

Lifehacker, Nov. 19, 2019.

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favorite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple.

LOCAL COMMUNITY EVENTS

1st
White Pine Stampede
http://whitepinestampede.org/

4th
TCNew Tech
https://tcnewtech.org/
AAUW TC Branch Mtg.
https://traversecityarea-mi.aauw.net/

6th
“Maiden” Fundraiser for YWIS
https://schoolship.org/news-events/maiden/

9th
North American VASA 44th Annual Festival of Races
http://www.vasa.org/
Academy Awards Party Benefit for State/ Bijou Theater
https://www.stateandbijou.org/

10th
G.T. Humanists Presents Deb Lake From American Waste
https://gthumanists.org/

12th
Traverse City Cannabiz Connection Networking Mixer
https://www.cannabizconnection.com/

15th
WinterLochen
https://www.interlochen.org/

20th
Grand Traverse ISSA Happy Hour
https://tc-issa.site/

21st-23rd
Young Farmer Leaders Conf.
https://www.michfb.com/mi/

22nd
7th Annual Guns and Hoses Benefit Hockey Game
Facebook.com/gtgunsnhoses/

23rd
Remembering Pasty Cline City Opera House Benefit
https://www.cityoperahouse.org/

23rd-29th
2020 Traverse City Restaurant Week

CALENDAR RESOURCES:
Google.com/traverse city events
TC Ticker Calendar
Traverse City Area Chamber
Events-My North
TraverseCity.com

4 E-mails You Should NEVER Open

No matter how “bomb-proof” we make your network, you and your employees can still invite a hacker in if you click on a link or open an attachment in an e-mail sent by a cybercriminal. Most spam is cleverly designed to sneak past all the filters and trick the recipient into opening the door. This still is the #1 way hackers circumvent firewalls, filters and antivirus, so it’s critical that you and your employees know how to spot a threatening e-mail. Here are four types of e-mails to look for:

The Authority E-mail. The most common phishing e-mails are ones impersonating your bank, the IRS or some authority figure. The rule of thumb is this: ANY e-mail that comes in where 1) you don’t PERSONALLY know the sender, including e-mails from the IRS, Microsoft or your “bank,” and 2) asks you to “verify” your account should be deleted. Remember, ANY important notification will be sent via old-fashioned snail mail. If it’s important, they can call you.

The “Account Verification” E-mail. Any e-mail that asks you to verify your password, bank information or login credentials, OR to update your account information, should be ignored. No legitimate vendor sends e-mails asking for this; they will simply ask you upon logging in to update or verify your information if that’s necessary.

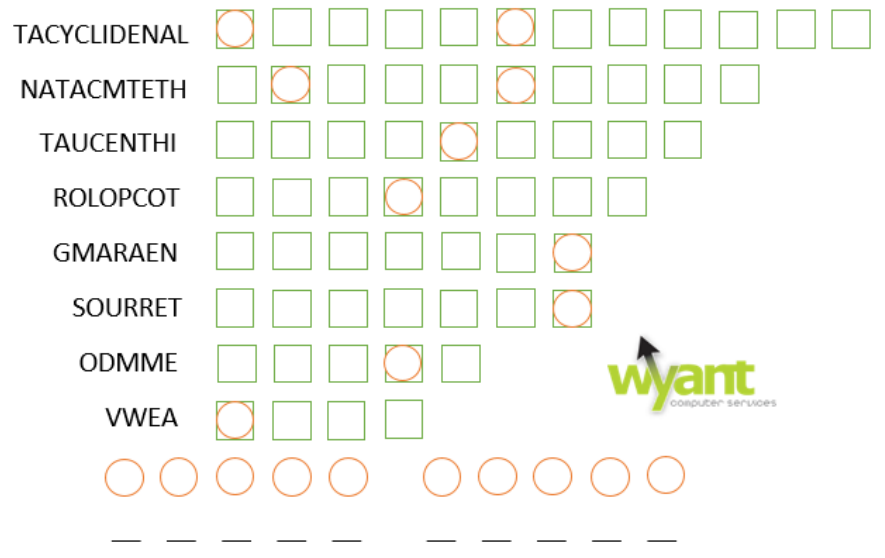
The Typo E-mail. Another big warning sign is typos. E-mails coming from overseas (which is where most of these attacks come from) are written by people who do not speak or write English well. Therefore, if there are obvious typos or grammar mistakes, delete it.

The Zip File, PDF Or Invoice Attachment. Unless you specifically KNOW the sender of an e-mail, never, ever open an attachment. That includes PDFs, zip files, music and video files and anything referencing an unpaid invoice or accounting file (many hackers use this to get people in accounting departments to open e-mails). Of course, ANY file can carry a virus, so it’s better to delete it.

WYANT WORD SCRAMBLE

*CONGRATS to Brittany Maggrett from Castle Farms for winning last month’s *Gift Card Drawing!*

January’s Answers: INTERRUPTION, INFLUENTIAL, MOMENTUM, BEHIND, DISTRACTIONS, COMPLANCENT, INSIGHT, GAZE Bonus: COMFORT ZONE



TACYCLIDENAL
NATACMTETH
TAUCENTHI
ROLOPCOT
GMARAEN
SOURRET
ODMME
VWEA

Bonus Clue: SUGARY ORGAN

***Email: wendy@gowyant.com the Answers for a chance to WIN A GIFT CARD!**

wyant computer services

1760 Forest Ridge Drive Ste. A
Traverse City, MI 49686

Inside February's News Letter!

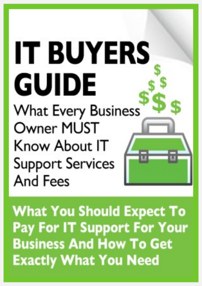
Top Tips: Password Security for Your Small Business

Put a greater emphasis on passwords. As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything.

Stop password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA).
MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security. *Small Business Trends, Nov. 1, 2019.*

Free Report Download: The Business Owner's Guide To IT Services And Fees



IT BUYERS GUIDE

What Every Business Owner MUST Know About IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Business And How To Get Exactly What You Need

You'll learn:

- **The three most common ways IT companies charge for their services and the pros and cons of each approach.**
- **A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.**
- **Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.**
- **How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.**

Claim your FREE copy today at https://www.gowyant.com/itbuyersguide