



VPNS ARE NOT AN INVISIBILITY CLOAK




(Don't Use Them Like One)

A virtual private network (VPN) is essential for modern office work to create a secure, encrypted connection between your device and a remote server, allowing you to work from anywhere while protecting sensitive data. VPNs are also gaining popularity for personal browsing by routing Internet traffic through a remote server to mask your IP address. It's like a gated tunnel only you can enter, which is handy for accessing region-restricted streaming services or content and protecting data when using public WiFi.


However, some people confuse VPNs with an invisibility cloak, believing that anything they do online while using a VPN is hidden. That is not the case. Some VPN services log your data (which can be leaked, hacked or sold), and there are other ways cybercriminals can track you online. Understand what VPNs do and don't do so you aren't putting yourself at unnecessary risk.



What VPNs Do (And Don't Do)

VPNs are excellent for enhancing privacy and security. **They DO:**

-  Hide your IP address, making it harder for websites and advertisers to track your online activities.
-  Encrypt your Internet traffic, safeguarding sensitive information like passwords and business communications.
-  Allow access to geo-restricted content, which can be beneficial for business research or accessing region-specific services.

Despite these advantages, VPNs have limitations. **They DON'T:**

-  Make you completely anonymous. While your IP address is hidden, websites can still track you using cookies and other tracking methods.

-  Protect you from malware or phishing attacks. A VPN cannot filter malicious content, so you still need robust antivirus software and cyber security practices.
-  Prevent all data logging. Some VPN providers may log your data, so choose one with a strict no-logs policy.

Warning: Avoid Free VPNs!

Free VPNs are dangerous. Many free services log your data and sell it, undermining the very privacy you're trying to protect. Free VPNs may also have weaker encryption standards, exposing you to more risks. Always opt for reputable VPN providers with clear privacy policies and transparency about how they use your information.

How To Use A VPN Responsibly

- **Choose A Reputable Provider:** Look for VPN services with strong privacy policies, good reviews and transparency about their data-handling practices.
- **Enable Kill Switch:** This feature ensures your Internet connection is severed if the VPN connection drops, so your data won't be leaked.
- **Update Regularly:** Keep your VPN software updated to benefit from the latest security improvements.
- **Combine With Other Security Steps:** To maximize protection, use a VPN with antivirus software, firewalls and good cyber security hygiene.

Understanding VPN capabilities and limitations ensures you use them effectively and responsibly, protecting your data without relying on a false sense of invisibility.



INSIDE THIS ISSUE

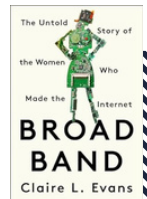
Hackers Are Targeting Small Construction Companies And Other Invoice-Heavy Businesses **P. 1**

The Business Owner's Guide To IT Support Services And Fees **P. 2**

Ignite Durham: School Supply Drive Update **P. 3**

BROAD BAND

By Claire L. Evans



In tech, there are stories we hear all too often: a major company got hacked, Meta dealing with yet another lawsuit or Google implementing some new security measure. However, there's one story we don't hear enough: pioneering women in tech. Much like *Hidden Figures* and *Rise of the Rocket Girls*, *Broad Band* by Claire L. Evans uncovers the pivotal yet overlooked contributions of female pioneers who shaped the Internet.

Evans vividly narrates the achievements of visionaries like Grace Hopper and Elizabeth "Jake" Feinler, showcasing their revolutionary work in computing and online networks. Evans sheds light on these hidden figures, inspiring a new generation to recognize and celebrate the women behind technological advancements. *Broad Band* is an essential, enlightening read that helps redefine the true history of technology.

THE ATTITUDE CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

Welcome The Attitude Chronicle. We are excited to bring this monthly publication to our clients and the Eastern Ontario business community. Each month we focus on tips to help your business run safely, securely and more profitably.

Small businesses are the backbone of our local economy, and it is extremely hard for them to recover from data breaches and other cyber attacks.

Our hope is that YOU never experience the loss of revenue, trust, and reputation that comes with a cyber incident. However, in today's risk climate, there's a higher chance of your organization facing a cyber incident than not.

We want to make sure you are brilliantly prepared.



HACKERS ARE TARGETING SMALL CONSTRUCTION COMPANIES AND OTHER INVOICE-HEAVY BUSINESSES

From 2023 to 2024, attacks on construction companies doubled, making up 6% of Kroll's total incident response cases, according to the 2024 Cyber Threat Landscape report from risk-advisory firm Kroll. Experts at Kroll note that the uptick could be driven by how work is carried out in the industry: employees work with numerous vendors, work remotely via mobile devices and operate in high-pressure environments where urgency can sometimes trump security protocols. All of these factors make the construction industry ripe for a cyber-attack.

Kroll. These e-mails look like document-signing platforms or invoices to socially engineer users into giving away information.

These tactics are having a higher success rate in smaller construction companies for a few reasons:

- **They deal with a lot of suppliers and vendors.** Construction companies work with many suppliers and vendors, and each vendor can be a weak spot that hackers can exploit. For example, if a hacker gets control of a vendor's e-mail, they can send fake invoices that look real, tricking businesses into sending money to the hacker's account instead. Multiply that by the number of vendors you work

continued on page 2...



This monthly publication is provided courtesy of Brandon Jones, CEO of Attitude IT.

OUR MISSION:

We're on a mission to protect 10,000 Ontario businesses from data loss and cyber-attacks.

Yours could be next.

Ripe For Hackers

Business e-mail compromise (BEC) – fake e-mails designed to trick employees into giving away money or sensitive information – made up 76% of attacks on construction companies, according to

...continued from cover

with, and that's a lot of potential entry points for a hacker.

- They use frequent mobile sign-ins. As truly remote workers, construction employees rely on mobile devices to sign into accounts and communicate from anywhere. This mobile accessibility, while convenient, also increases the risk because mobile devices are typically less secure than desktops or laptops.
- They work in a high-stakes, high-pressure environment. In industries where delays can be costly, such as construction or health care, employees may rush to process invoices or approve transactions without thoroughly verifying their legitimacy. This urgency is precisely what attackers count on to get around standard security checks.

Your Industry Could Be Next

Construction companies are not the only ones experiencing more attacks. Small manufacturing companies, higher education institutions and health care providers that lack the robust security infrastructure of larger industry players are also examples of industries seeing a rise in cyber-attacks. These industries, like construction, deal with numerous vendors

and urgent invoices, making them prime targets for business e-mail compromise and invoice fraud.

How To Protect Against BEC And Invoice Fraud

1. Use Multifactor Authentication (MFA)

Accounts that use MFA are 99% less likely to be attacked, according to the Cybersecurity and Infrastructure Security Agency. MFA requires multiple forms of verification before granting access to sensitive information. Even if hackers obtain log-in details, they can't access accounts without the second credential, typically a mobile device or a biometric scan.

2. Always Verify Supplier Information

One of the simplest yet most effective measures is to verify the authenticity of invoices and supplier information. Establish a protocol where employees are required to double-check the details of any financial transactions directly with the supplier through a known and trusted communication channel, such as a phone call.

3. Keep Employees Trained On Common Attacks

Employee training is a vital component of a comprehensive cyber security strategy. Regular training sessions on recognizing social engineering and phishing attempts and understanding the importance of following

verification protocols can empower employees to act as the first line of defense. The Information Systems Audit and Control Association recommends cyber security awareness training every four to six months. After six months, employees start to forget what they have learned.

4. Maintain Strong Cyber Security Practices

Cybercriminals regularly exploit outdated software to gain entry into systems. Small businesses can close these security gaps by keeping software up-to-date. Investing in robust antivirus and anti-malware solutions can help detect and stop attacks before they get into your systems.

You're A Target, But You Don't Need To Be A Victim

Hackers are increasingly targeting small, invoice-heavy industries like construction, manufacturing and health care due to their inherent vulnerabilities. By understanding the reasons behind these attacks and implementing robust cyber security measures, small business leaders can protect their organizations from becoming easy targets. Utilizing MFA, maintaining strong cyber security practices, verifying supplier information and training employees are essential to stopping attacks.



IGNITE DURHAM



Back in July we started a school supply drive in partnership with Ignite Durham.

Ignite Durham is a non-profit organization that helps provide students and teachers with school supplies including; healthy snacks, math and reading materials, classroom supplies. It is operational year round.

We had the opportunity to do a tour with Brandon and Emily Collins and we're blown away by what the organization has accomplished and we are so excited to become more involved with Ignite and offer further support for students in the Durham District.

With the help of our partners Field Effect and UPS store 54 in Whitby we were able to donate over \$1,254 directly to students in the Durham region. How Amazing is that? Thank you to everyone who helped us make this a success!

For more information on Ignite Durham, visit <https://ignitedurhamlearningfoundation.ddsbc.ca>

DON'T FORGET TO CHANGE NEW-HIRE PASSWORDS

To keep things simple, employers often create easy, temporary passwords for new hires to log in to accounts or devices during their first few days. However, a Specops analysis of millions of passwords found that 120,000 used common words related to new employees, meaning the new-hire passwords were never changed. Hackers know this and use these simple password structures in brute force attacks. The most commonly compromised passwords on new accounts are user, temp, welcome, change, guest, starter, logon and onboard. Look familiar?

Prevent this mistake by forcing change at log-in (if possible), using a service like First Day Password or an authenticator app or making a new-hire password REALLY hard.

Upcoming Events:

Scan the QR code to register, or visit WhitbyChamber.org

ATTITUDE IT
Keeping Your Technology On Course

THE 2024 WHITBY JOB FAIR

Are you ready to take the next big step in your career journey? Exciting opportunities await you at The 2024 Whitby Job Fair!

10:00 AM to 4:00 PM | September 14, 2024

Abilities Centre | 1 Jim Flaherty Street, Whitby

WE ARE HIRING!

We will be in attendance at the Whitby Job Fair on September 14th. We love supporting these events and are always on the lookout for local talent.

CARTOON OF THE MONTH

