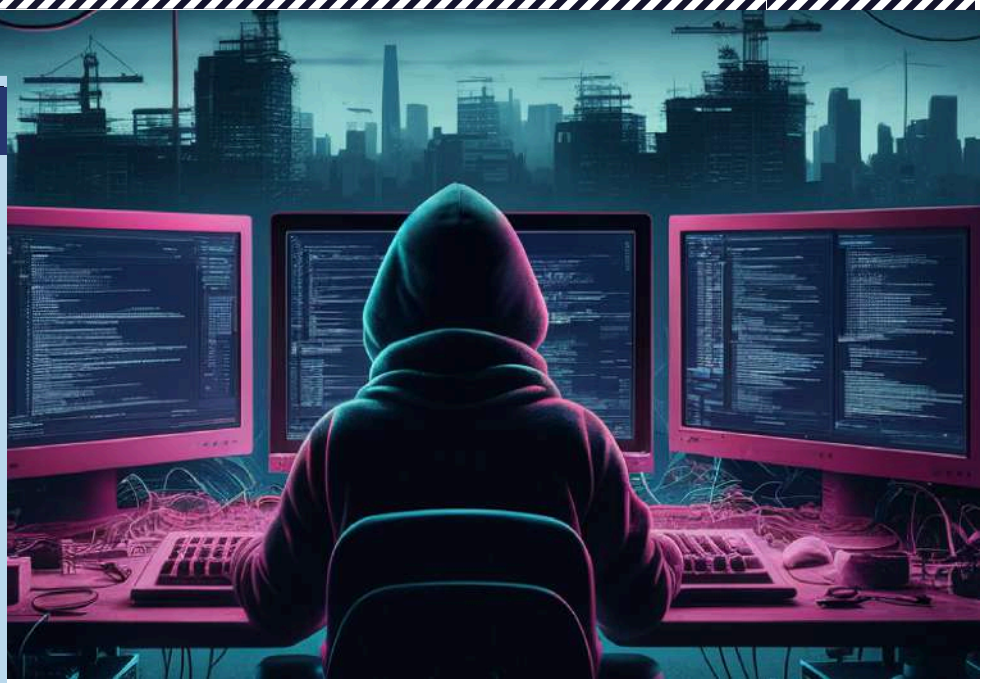
THE TECH CHRONICLE

Insider tips to make your business run faster, easier and more profitably



THIS MONTH

We're delighted to invite you to the **Official Launch of ERGOS Shield**, which will take place from 12 to 4pm on Friday, October 18th. The invitation is open and valid for all!

What to expect:

- Wine tasting session
- Complimentary lunch with a great view
- A goodie bag full of useful ERGOS stuff
- Special talks by renowned cybersecurity experts
- and a valuable networking opportunity!

Learn more and RSVP on our webpage by **the end of September:** https://ergos.uk/ergos-shield-ergos-shield/. We're looking forward to seeing you there!

This monthly publication is provided courtesy of Gino Choucair, CEO of ERGOS.

OUR MISSION:

Ensuring your technology success, securely & simply.

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.

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 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...

...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 recognising 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.

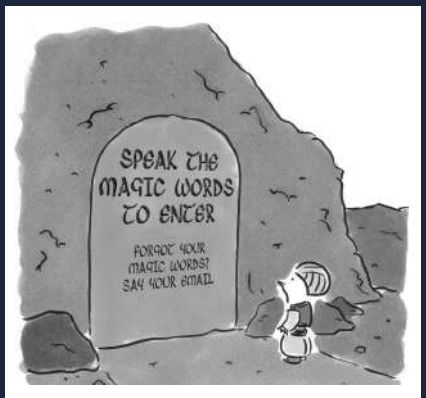
4. Maintain Strong Cyber Security Practices

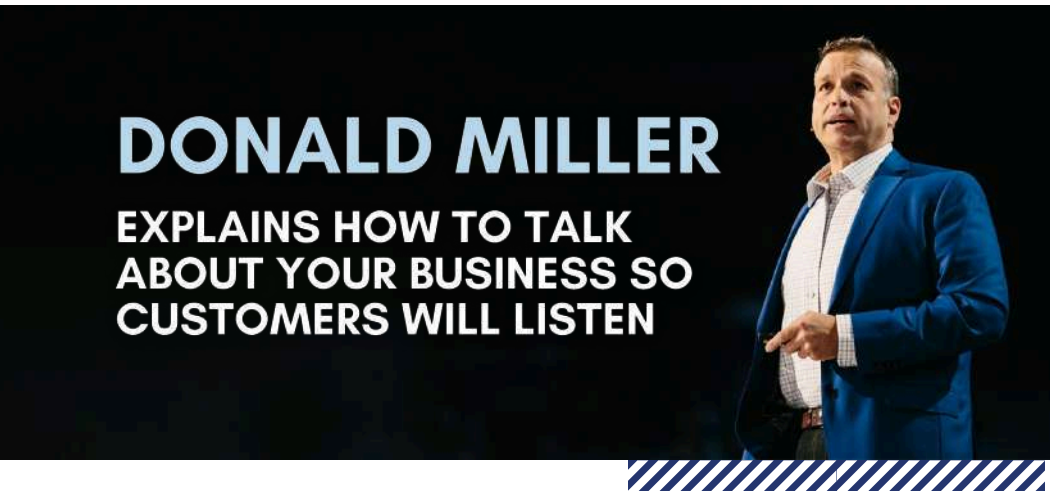
Cybercriminals regularly exploit outdated software to gain entry into systems. Small businesses can close these security gaps by keeping software up-to-date. Investing in robust antivirus and anti-malware solutions can help detect and stop attacks before they get into your systems.

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. Utilising MFA, maintaining strong cyber security practices, verifying supplier information and training employees are essential to stopping attacks.

CARTOON OF THE MONTH





It's really, really hard to grab people's attention today. Customers are busy and inundated with choices, making it hard for businesses to stand out. Donald Miller empathises. He knew people loved his book *Building A Story Brand* – after all, he sold millions of copies. But when Miller decided to tour and fill 700 theatre seats for a speaking engagement, half remained empty. "I learned that I'm good at writing the 300 pages but not very good at writing the sentence that makes you want to read the 300 pages. It's two different skill sets," Miller explained to business leaders at a recent industry conference.

Do you know how to communicate the value of your products or services so customers buy again and again? Most of us don't. That's because we prioritize creativity and cleverness over clarity. Miller argues that no dollar spent on branding, colour palettes, logos or website redesigns will help if you aren't clear about your message. Why? Because human brains are hardwired for two things:

1. **Survive And Thrive**
2. **Conserve Calories**

We don't have time or energy to process unnecessary information; we only buy what helps us get ahead. "If you confuse people about how you can help them survive, you'll lose," Miller says.

Tell A Story

"The first thing we have to understand is that people buy products only after reading words or hearing words that make them want to bother to buy those products," Miller explains.

Let's say you meet two people at a cocktail party who do the same thing for a living. You ask person A, "What do you do?" They say, "I'm an at-home chef." So, you ask questions about where they went to school, their favourite recipes, etc. Then, you meet person B and ask the same thing. They respond, "You know how most families don't eat together anymore? And when they do, they don't eat healthy? I'm an at-home chef."

Who does more business? Person B, because they told a story about how they solved a problem. Humans love stories; it's why we binge-watch good television. Good stories have the same core structure, and Miller explains how you can use it to tell the story of why your business is the one customers should choose.

Identify your hero's (customer's) problem and talk about it a lot. When someone asks, "What do you do?" don't tell them. Start by describing the problem. Spend 75% of your time talking about your customer's problem because that triggers the purchase.

Introduce them to the guide (you). The key to being a guide is to listen: "I'm sorry you're going through that. It sounds very stressful." Then, be competent: "I feel your pain, and I know how to get you out of this hole."

Give them a plan. This is an active call to action, like "Buy now" or "Schedule a call." You must challenge the hero to take the action that leads to success.

Remember, the story you're telling is not about you. It's about your customer, the hero. Once you have your message, distill it into short, simple and repeatable sound bites. "It works every single time," Miller says, "because the human brain cannot ignore a story."

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.

CLIENT SPOTLIGHT:

COVENEY NICHOLLS CHARTERED ACCOUNTANTS

"Deep, long-term relationships matter to us – sometimes lasting not just years or decades but for generation after generation. ERGOS helps us provide reliable, fast service to our own clients and really reflects how we want to do business"

Would you like your company highlighted here? Contact your Account Director or call us at 020 3818 3411.