WHY PHISHING ATTACKS SPIKE IN THE SUMMER

You and your employees may be getting back from vacation, but cybercriminals never take a day off. In fact, data shown in studies from vendors ProofPoint and Check Point indicate that phishing attempts actually spike in the summer months. Here's how to stay aware and stay protected.

Why The Increased Risk?

Attackers use your summer travel bug to their advantage by impersonating hotel and Airbnb websites, says Check Point Research. They've uncovered a sharp increase in cyberthreats related to the travel industry – specifically, a 55% increase in the creation of new website domains related to vacations in May 2025, compared to the same period last year. Of over 39,000 domains registered, one in every 21 was flagged as either malicious or suspicious.

August/September is also back-to-school time, which means an uptick in phishing attempts imitating legitimate university e-mails, targeting both students and staff.

While these threats might not affect your industry directly, there's always a chance that employees pursuing their master's degree or planning a vacation will check their personal e-mail on their work computer – and it takes only one wrong click for cyberattackers to have access to all of your business's data.

What To Do About It

While AI is making cybersecurity stronger and workflows smoother, it's also making phishing attacks more convincing. That's why it's important to train yourself and your team on what to look for, to avoid clicking on a malicious link.

Safety tips to prevent attacks:

- **Keep an eye out for shady e-mails.** Don't only check for misspellings and poorly formatted sentences in the body of e-mails; AI can write e-mails for attackers just like it can for you. Also examine the e-mail address of the sender and the text of the link itself, if visible, to make sure everything looks legitimate.
- **Double-check URLs.** Misspellings in the link text or unusual domain endings, like .today or .info, can be an indicator of an attack. Domain endings like these are often used in scam sites.
- **Visit websites directly.** It's always better to search for the website yourself, rather than clicking on links in any messages or e-mails.
- **Enable Multifactor Authentication (MFA).** Setting up MFA ensures that even if a breach does occur within your company, your login credentials will remain protected – and so will any data secured behind them.
- **Be careful with public WiFi.** If you need to use public WiFi, use a VPN for additional protection when accessing secure information, like booking portals or bank accounts.
- **Don't access personal e-mail on company devices.** Accessing personal e-mail, messaging or social media accounts on business devices increases your risk. Keep personal accounts on your personal devices, and work-related accounts on the work devices.
- **Ask your MSP about endpoint security.** Endpoint detection and response (EDR) software can monitor your desktops and mobile devices, detect/block phishing attempts, malicious downloads and alert your MSP immediately in the event of a breach, limiting your data's exposure.

Phishing attempts become more sophisticated every day, and AI is only speeding that process along. Because of this, it's essential to keep your team well-informed of the risks; knowledge is the best defense against phishing attacks. Stay informed and stay safe!

Connectability Corner
PUTTING THE PIECES TOGETHER.
Powered by: Connectability
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

IS YOUR BUSINESS TRAINING AI TO HACK YOU?

There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write e-mails, summarize meetings and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems – especially when it comes to your company's data security.

Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by *Tom's Hardware*.

Now picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside e-mails, transcripts, PDFs or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't.

In short, the AI helps the attacker – without knowing it's being manipulated.

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools on their own, often with good

continued on page 2...

...continued from cover

intentions but without clear guidance. Many assume AI tools are just smarter versions of Google.

They don't realize that what they paste could be stored permanently or seen by someone else.

And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control.

Here are four steps to get started:

1. Create an AI usage policy.

Define which tools are approved, what types of data should never be shared and who to go to with questions.

2. Educate your team.

Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

3. Use secure platforms.

Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.

4. Monitor AI use.

Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay.

Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble.

A few careless keystrokes can expose your businessto hackers, compliance violations, or worse.

Earn $1,000 by Referring a Business to Us!

We know that great businesses are built on strong connections, and we'd love your help connecting with organizations that need reliable IT support. To show our appreciation, we're offering $1,000 for every qualified referral - even if they don't become a client!

How It Works:
1. Refer a business with 10+ computer users in the GTA.
2. Make an introduction via phone or email.
3. If they book and attend a Free IT Cybersecurity Risk Assessment, you earn $1,000 - no strings attached.

Who Makes a Great Referral?
We're looking to connect with CEOs, Executive Directors, or IT Managers in any industry that relies on technology. Some great examples include financial services, real estate, professional services, property management, wholesale distribution, and manufacturing - but any growing business with IT needs is a great fit!

Know Someone? Let's Make It Easy!
Whether it's a client, vendor, or colleague, simply introduce us, and we'll take it from there.
We're even happy to co-host a webinar, seminar, or special offer for any business groups you belong to.

OUR REFERRAL PROGRAM

A failed 2001 draft led former Oakland A's General Manager Billy Beane to overhaul how he managed talent—sparking a transformation that revolutionized baseball and inspired industries worldwide.

Using a data-driven strategy, Beane turned the low-budget Oakland A's into consistent playoff contenders. The team won seven American League Western Division titles and made 10 postseason appearances, all while operating with one of the lowest payrolls in Major League Baseball.

Beane's approach, known as the "Moneyball" philosophy, emphasized objective analysis over tradition and intuition. It gained widespread recognition through a best-selling book and Oscar-nominated film chronicling his unconventional path to success.

At a recent leadership event, Beane outlined how businesses can adopt similar principles to build high-performing teams despite resource limitations.

Make Data-Backed Decisions

"Baseball had been tracking stats since the 1800s, but none of it influenced decision-making," Beane said. "I turned running a team into a math equation." He replaced gut instinct and subjective scouting with analytics, reshaping how talent was evaluated.

Identify Undervalued Assets

"There's a championship team you can afford—you just need to find what others undervalue," Beane explained. He focused on on-base percentage, a metric more predictive of winning than traditional stats, uncovering overlooked players who delivered strong results.

Be Relentless With Execution

"You can't go back and forth," Beane said. "If you commit to data, you have to use it every time." His team stayed disciplined throughout each season, trusting the math to guide decisions rather than reacting emotionally to short-term outcomes.

Maximize The Middle

Rather than spending big on stars, Beane focused on building depth. "We couldn't afford top players, so we made sure we didn't have bad ones," he said. "A strong middle roster outperforms one with gaps."

Hire Differently

Beane recruited talent from outside traditional pipelines. One example was hiring a Harvard economics major as assistant GM—unusual in a role typically filled by former players. This fresh thinking helped the A's stay ahead.

Redefine Culture With Data

"If we did what everyone else was doing, our results would match our budget," Beane said. "We challenged the norm, used data to value skills differently and changed our outcomes."

Lead With Transparency

"Data explains decisions," he noted. "Even when you're not always right, clarity builds trust."

Level The Playing Field

Beane's philosophy proves that success isn't solely dictated by budget. With innovation, discipline and a data-first approach, even smaller organizations can compete with giants.

As he put it: "Data isn't an opinion. It's a fact."

CYBERSECURITY TOOL OF THE MONTH

Pentesting: Expose Weaknesses Before Hackers Do

Pentesting is a simulated cyberattack on your systems to uncover vulnerabilities before real attackers exploit them. Security experts test your defenses, identify gaps, and provide actionable fixes – giving you a clear picture of how resilient your environment really is.

Why It Matters

- Hackers use the same techniques – beat them at their own game
- Compliance standards (PCI, HIPAA, SOC 2, etc.) often require regular pentests
- Reveals blind spots that routine scans and tools miss
- Protects your reputation by preventing breaches before they happen

Monthly Charity Donation

childcan
Facing Childhood Cancer Together

September is Childhood Cancer Awareness Month. This month, we are proud to support Childcan, a Canadian charity providing vital programs and services for children with cancer and their families.

From funding research to offering direct support, Childcan helps families navigate the toughest challenges with care, compassion, and hope. Together, we can shine a light on childhood cancer, stand with affected families, and contribute to a future with better treatments and brighter outcomes.