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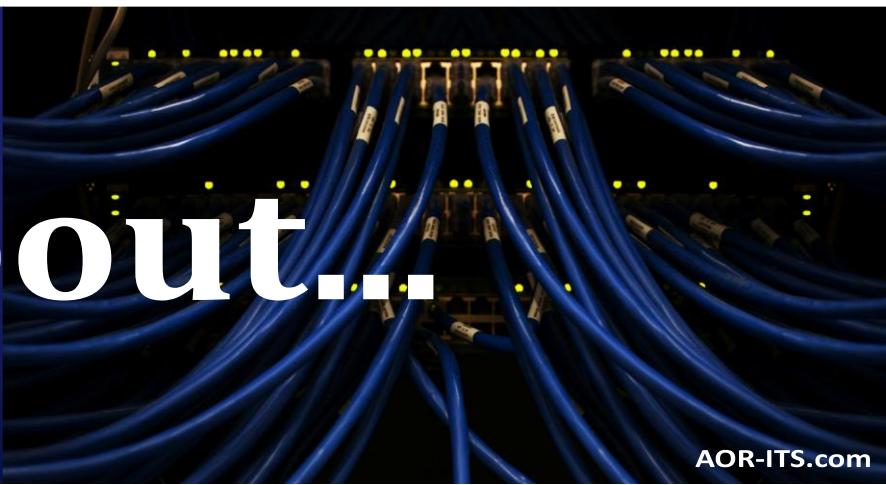
You and your employees may be getting back from vacation, but cybercriminals never take a day off. In fact, data shown in studies from vendors ProofPoint and Check Point indicate that phishing attempts actually spike in the summer months. Here's how to stay aware and stay protected.

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.

Late summer 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 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 in 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, such as ".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 and block phishing attempts and malicious downloads, and alert your MSP immediately in the event of a breach, drastically 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!

Start the season secure – book your FREE Cybersecurity Assessment today.

Click here to book your [FREE Cybersecurity Assessment](#) now.

Questions? Call our Glenside, PA office today at 267-699-2551. Or visit us on the web at [AOR-ITS.com](#) to learn more about our proven managed IT solutions, including cybersecurity, for small local businesses.