Cyber-espionage is a type of cyber-attack that involves an unauthorised user (or multiple users) accessing a victim’s sensitive information in order to secure economic benefits, competitive advantages or political gain. Also known as cyber-spying, the primary targets of such cyber-attacks include government entities, large corporations and other competitive organisations.

Understanding Cyber-espionage

**Best Practices to Keep Routers Secure**

Most homes and offices have a router that provides internet access to multiple devices within the same space. Unfortunately, cyber-criminals may target routers because they can steal data or alter a router’s ability to recognise illegitimate websites, putting users and their organisations at risk. Employees working from home may be particularly vulnerable to cyber-attacks via routers. As such, it’s important for organisations to share the following best practices with staff:

**Best Practices to Keep Routers Secure**

Most homes and offices have a router that provides internet access to multiple devices within the same space. Unfortunately, cyber-criminals may target routers because they can steal data or alter a router’s ability to recognise illegitimate websites, putting users and their organisations at risk. Employees working from home may be particularly vulnerable to cyber-attacks via routers. As such, it’s important for organisations to share the following best practices with

Cyber-criminals may leverage cyber-espionage to gather classified data, trade secrets or intellectual property from their victims—which can be sold for profit or used to expose organisations. Cyber-espionage has become a rising concern over the past few years. In fact, the UK’s Government Code and Cipher School estimates there are 34 separate nations that have professional well-funded cyber-espionage teams. With this in mind, it’s crucial that your organisation understands cyber-espionage tactics and takes measures to mitigate such incidents.

Cyber-criminals may engage in a variety of tactics to execute cyber-espionage, such as:

* Exploiting security vulnerabilities in websites or browsers
* Utilising phishing scams
* Bribing actual employees or contractors to share a target’s sensitive information in exchange for payment
* Injecting different forms of malware (eg Trojans and worms) within updates from third-party software applications

Safeguard your organisation’s operations from cyber-espionage by implementing strong cyber-security measures, including:

* **Educating employees**—Train employees on cyber-espionage and related prevention tactics, including phishing awareness and password management.
* **Protecting critical data**—Encrypt and store all critical data in safe, secure locations.
* **Restricting access**—Only permit employees to access technology and data when it’s specifically needed to perform their duties. Additionally, require multifactor authentication whenever possible.
* **Leveraging sufficient software**—Protect all workplace technology (and the data stored on it) with proper security software, including endpoint detection tools, antivirus programs and firewalls.

Finally, it’s critical to secure adequate insurance to help protect against losses from cyber-espionage and other attacks. Contact us today for further risk management guidance.

Traditional cyber-security protocols often can’t keep up with the rapidly evolving nature of modern workplaces. In particular, the complexity of hybrid work arrangements, the rising number of fully remote employees and the dramatic increase in the use of cloud-based systems may make traditional perimeter security ineffectual. Fortunately, a new security model, known as “zero trust,” can help keep corporate networks safe.

**Best Practices to Keep Routers Secure**

Most homes and offices have a router that provides internet access to multiple devices within the same space. Unfortunately, cyber-criminals may target routers because they can use them to steal data, or they may alter a router’s ability to recognise illegitimate websites, putting users and their organisations at risk. Employees working from home may be particularly vulnerable to cyber-attacks via routers. As such, it’s important to share the following best practices with staff:

* Do not use default passwords or wireless network names that the router came with.
* Turn on wi-fi protected access.
* Disable the service set identifier to prevent the wireless network from being easily seen.
* Keep the router’s firmware up to date.
* Establish a network for guest users.
* Disable wi-fi protected setup.
* Routinely restart the router to clear the system’s memory and refresh connections.
* Disable remote accessibility.
* Make sure every router administrator has their own username, password and proper access privileges.
* Monitor network activity regularly.

Contact us today for further resources on cyber-security best practices.

The Zero-trust Model Explained

Rather than trusting the identity and intentions of users within an organisation, a data breach is presumed with every request under a zero-trust approach. Consequently, every access request must be authenticated and authorised as if it originated from an open network. As such, a zero-trust model can help reduce an organisation’s attack surface area and prevent lateral movement—where attackers are able to move freely within the organisation’s perimeter once access is gained. This is especially important, seeing as lateral movement was observed in 25% of all attacks, according to a recent global report by cloud computing company VMware.

Consider these tips for adopting a zero-trust approach in your organisation:

* **Define the attack surface**. To adopt a zero-trust framework, your organisation’s critical data, assets, applications and services must be identified. This critical information forms a “protect surface,” which is unique to every organisation.
* **Create a directory of assets**. Determine where your sensitive information lives and who needs access to it. Additionally, understand how many user accounts your organisation has and where these connect. Consider removing old accounts and enforcing mandatory password rotation measures.
* **Adopt preventive measures**. Give users the least amount of access necessary to do their work and use multifactor authentication to verify accounts. Also, establish micro-perimeters to act as border control within the system and prevent unauthorised lateral movement.
* **Monitor continuously.** Inspect, analyse and log all data and consider analytics to improve visibility and enhance defences. Further, make sure your organisation swifty escalates and stores logs with anomalous activity or suspicious traffic.

By adopting a zero-trust approach, your organisation can significantly reduce the risk of becoming a cyber-attack victim and better secure its network, applications and data.

Contact us today for additional risk management guidance and insurance solutions.