CYBER TERMINOLOGY

Adware	Adware's job is to create revenue for the developer by subjecting the victim to unwanted advertisements. Common types of adware include free games or browser toolbars. They collect personal data about the victim, then use it to personalize the ads they display. Though most adware is legally installed, it's certainly no less annoying than other types of malware.
Antivirus	Software used to prevent, detect and delete viruses or malicious software from a computer.
Botnets + DDOS	Botnets + DDOS - A botnet isn't a type of malware, but a network of computers or computer code that can carry out or execute malware. Attackers infect a group of computers with malicious software known as "bots," which are capable of receiving commands from their controller. These computers then form a network, providing the controller access to a substantial degree of collective processing power, which can be used to coordinate distributed denial of service (DDoS) attacks, send spam, steal data, and create fake ads on your browser
Bricking	Bricking causes a computer to become fully non-functional for its intended purpose.
Cloud Service Provider	Cloud Service Provider means any third party with whom the Insured has a written contract for the provision of computing services, infrastructure platforms or business applications. Cloud Service Provider does not include any Social Media Platform.
Cyber Extortion	Cyber Extortion Costs means the reimbursement of reasonable fees, costs and expenses incurred by the Insured, or paid on the Insured's behalf, with the prior written consent of the Insurer, such consent not to be unreasonably withheld, to terminate or mitigate any credible threat of a Business Interruption Event, Data Liability Event or Network Security Event resulting from an actual or attempted extortion by a third party.

Firewall	A network security device that monitors and filters incoming and outgoing network traffic.
Funds Transfer Fraud	Funds Transfer Fraud Event means the commission by any Third Party: (i) via Unauthorised Access leading to any unauthorised electronic transfer of the Insured's funds from the Insured's computer system or network due to the fraudulent manipulation of electronic documentation which is stored on the Insured's computer system; (ii) of theft of money or other financial assets from the Insured's corporate credit cards by electronic means; and / or (iii) of any phishing, vishing or other social engineering attack against the Insured that results in the unauthorised transfer of Insured's funds to a Third Party.
Malware	Malware is an umbrella term for any type of "malicious software" that's designed to infiltrate your device without your knowledge. There are many types of malware, and each works differently in pursuit of it's goals. However, all malware variants share two defining traits: they're sneaky, and they're actively working against your best interests. The vast majority of malware falls into the below basic categories, depending on how it functions.
PCI-DSS	PCI-DSS stands for Payment Card Industry – Data Security Standard.
Phishing	Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable source to induce individuals to reveal information, such as passwords and credit card numbers.
Ransomware	Ransomware is the malware version of a kidnapper's ransom note. It typically works by locking or denying access to your device and your files until you pay a ransom to the hacker. Any individuals or groups storing critical information on their devices are at risk from the threat of ransomware.
Spyware	Spyware collects information about a device or network, then relays this data back to the attacker. Hackers typically use spyware to monitor a person's internet activity and harvest personal data, including login credentials, credit card numbers or financial information, for the purposes of fraud or identity theft.

Trojans

Trojans - Ancient Greek poets told of Athenian warriors hiding inside a giant wooden horse, then emerging after Trojans pulled it within the walls of their city. A Trojan Horse is therefore a vehicle for hidden attackers. Trojan malware infiltrates a victim's device by presenting itself as legitimate software. Once installed, the Trojan activates, sometimes going so far as to download additional malware.

Worms

Worms are designed with one goal in mind: proliferation. A worm infects a computer, then replicates itself, spreading to additional devices while remaining active on all infected machines. Some worms act as delivery agents to install additional malware. Other types are designed only to spread, without intentionally causing harm to their host machines – but these still clog up networks with bandwidth demands

Visit www.forwardinsurance.ca for tips on selling cyber coverage, claims examples,

and to access the JET platform for instant Cyber Liability quotes and policy issuance.