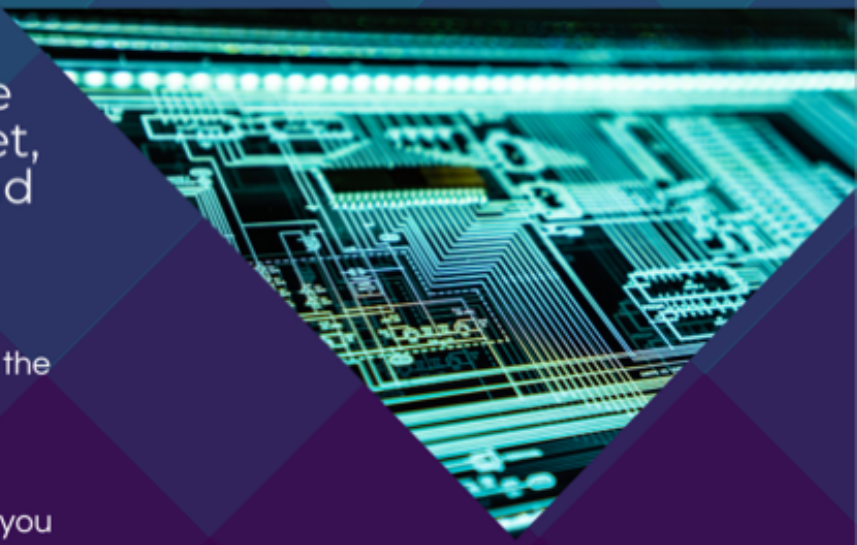
EVRON

TECH DEFINED

Cybersecurity Edition



As more devices become connected to the internet, concerns over privacy and security are growing.

There is a long list of terms related to cybersecurity that get thrown around in the articles you come across daily. Here are definitions of the ones that are most common + we think are most critical for you to understand.

MALWARE

This is a generic term to describe various forms of malicious software designed to exploit the vulnerabilities in a computer. This malicious software can be a virus, trojan, worm or ransomware.

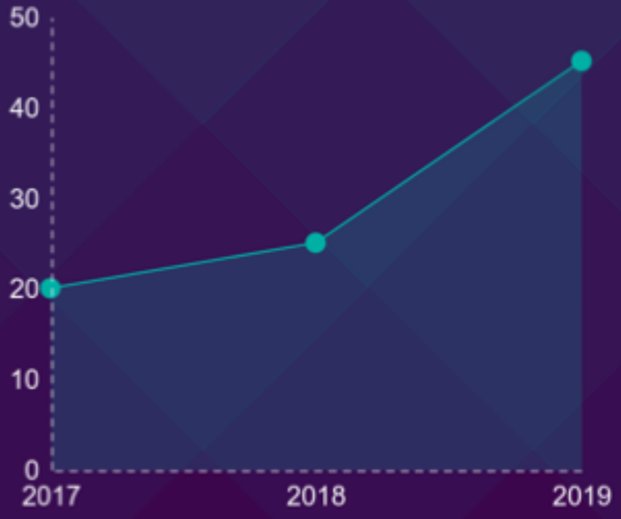
RANSOMWARE

This is a type of malware that locks or encrypts all the data files on your computer and demands a ransom be paid in order to have them unlocked or decrypted. It is truly holding your data hostage for a ransom.

$133K The average cost of ransomware to businesses

ZERO-DAY VULNERABILITY

Or zero-day attacks take advantage of a security vulnerability on the same day that the vulnerability becomes publicly known (zero-day). In other words, these attacks target vulnerabilities that are publicly known but no fix has yet been released.



ONGOING THREAT

The number of zero-day attacks have increased over the years and are predicted to continue to jump. Updating to Windows 10 and Office 365 can prevent some of these threats.

DDOS

Distributed Denial of Service, is a form of a cyber attack with the sole purpose to disrupt a server such as a web server or a web site. The attacker makes it unusable by “flooding” it with malicious traffic or data from multiple compromised computers launching a simulated flood of spurious requests to the target web site.

PHISHING

This is a sophisticated attack using social engineering to obtain sensitive information. This could be a personalized e-mail message designed to trick people into opening the e-mail and divulging personal or confidential data such as passwords and bank account information.

90%

of all breaches are Phishing scams

PATCH/UPDATE

A "Patch" is a set of updates to a computer program or operating system to fix or improve it. Security Patches fix security vulnerabilities and other bugs. Proper patch management prevents computers from missing updates and brings those that have missed them up to date.

BREACH

Event when a hacker successfully exploits a vulnerability in a computer or device and gains access to its data and network.

FIREWALL

This is like a gatekeeper or a perimeter defense between internet connection and client network. This could be a hardware or a software appliance.

EVRON

Evron takes a layered approach to security. A blend of several protections will keep your business secure. Talk to us if your business is one of the 53% of SMBs vulnerable to an attack.

info@evron.com | (905) 477-0444