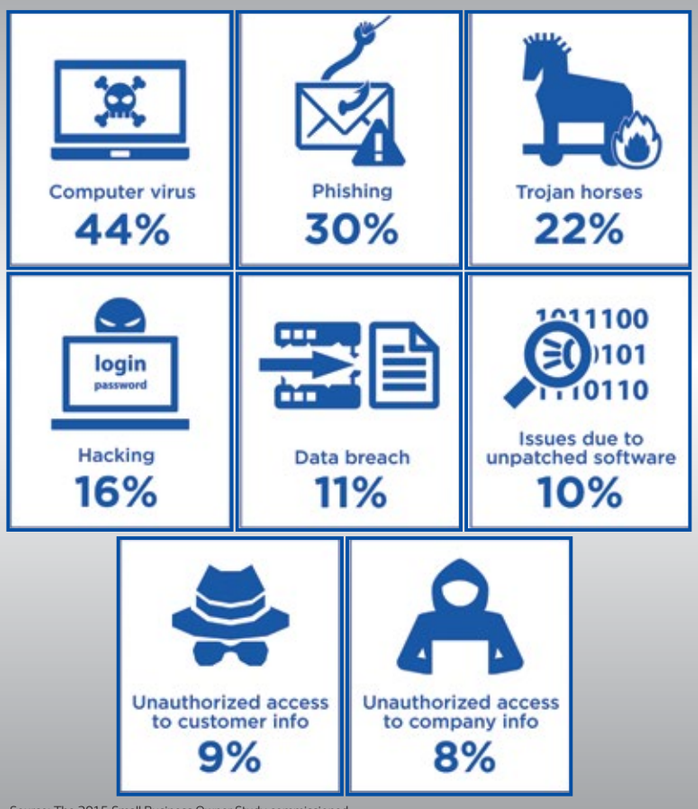
8 Types of Cyber Attacks
Your Business Needs to Avoid

Most small business owners **have been cyber victims**



Source: The 2015 Small Business Owner Study commissioned by Nationwide and conducted by Harris Poll Online.

Just as pollution was a side effect of the Industrial Revolution, so are the many security vulnerabilities that come with increased internet connectivity. Cyber-attacks are exploitations of those vulnerabilities.

For the most part unavoidable, individuals and businesses have found ways to counter cyber-attacks using a variety of security measures and just good ol' common sense. Regardless how safe a business feels it and its systems are, however, everyone must still be aware of and vigilant toward online threats.

Let's examine eight of the most common cyber-attacks that your business could face

- **Malware** is an all-encompassing term for a variety of cyber threats including Trojans, viruses and worms. Malware is simply defined as code with malicious intent that typically steals data or destroys something on the computer.
- **Phishing:** Often posing as a request for data from a trusted third party, phishing attacks are sent via email and ask users to click on a link and enter their personal data. Phishing emails have gotten much more sophisticated in recent years, making it difficult for some people to discern a legitimate request for information from a false one. Phishing emails often fall into the same category as spam, but are more harmful than just a simple ad.
- A **password attack** is exactly what it sounds like: a third party trying to gain access to your systems by cracking a user's password.
- A **Denial-of-Service (DoS)** attack focuses on disrupting the service to a network. Attackers send high volumes of data or traffic through the network (i.e. making lots of connection requests), until the network becomes overloaded and can no longer function.
- **"Man in the Middle" (MITM):** By impersonating the endpoints in an online information exchange (i.e. the connection from your smartphone to a website), the MITM can obtain information from the end user and the entity he or she is communicating with.
- **Drive-By Downloads:** Through malware on a legitimate website, a program is downloaded to a user's system just by visiting the site. It doesn't require any type of action by the user to download.
- **Malvertising:** A way to compromise your computer with malicious code that is downloaded to your system when you click on an affected ad.
- **Rogue Software:** Malware that masquerades as legitimate and necessary security software that will keep your system safe.

Cyberspace lies at the heart of modern society; it impacts our personal lives, our businesses and our essential services. Cyber security embraces both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or industrial espionage.

E-crime, or cyber-crime, whether relating to theft, hacking or denial of service to vital systems, has become a fact of life.

Cyber terrorism presents challenges for the future. We have to be prepared for terrorists seeking to take advantage of our increasing internet dependency to attack or disable key systems.

As with most types of crime, vigilance is one of the keys to prevention. As cyber criminals become more sophisticated and more transactions migrate online, the number of threats to people and businesses will continue to grow.

Prepare yourself and your business by taking the time to secure your systems and make cyber security a priority.

For Security Solutions:
Call: +919717495402
Email: contact.us@securitas-india.com

For Background Verification:
Call: +91 9978990585
Email: ev.screen@securitas-india.com

For Facility Management:
Call: +919582500587
Email: support@walsons.com

www.securitas.in
www.walsons.com