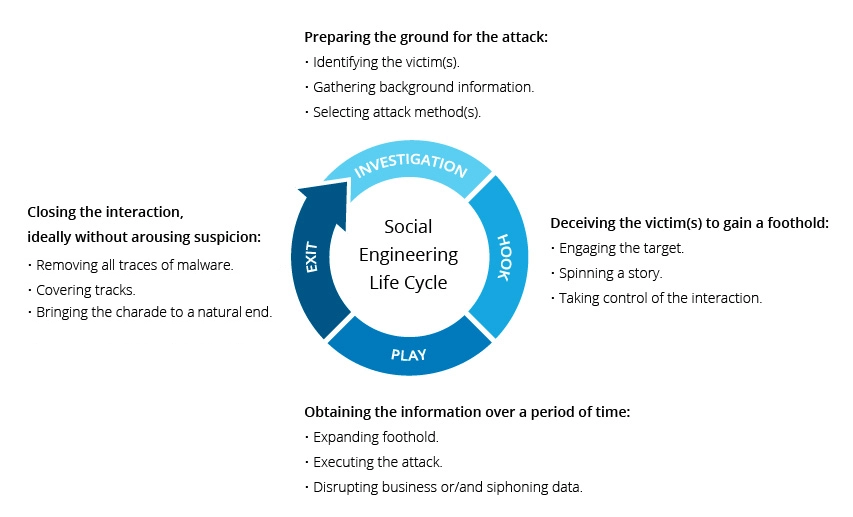
**Social engineering & Techniques**

**Social engineering** is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.



What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

* **Baiting**

As its name implies, baiting attacks use a false promise to pique a victim’s greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.

* **Scareware**

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraud ware.

* **Pretexting**

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

* **Phishing**

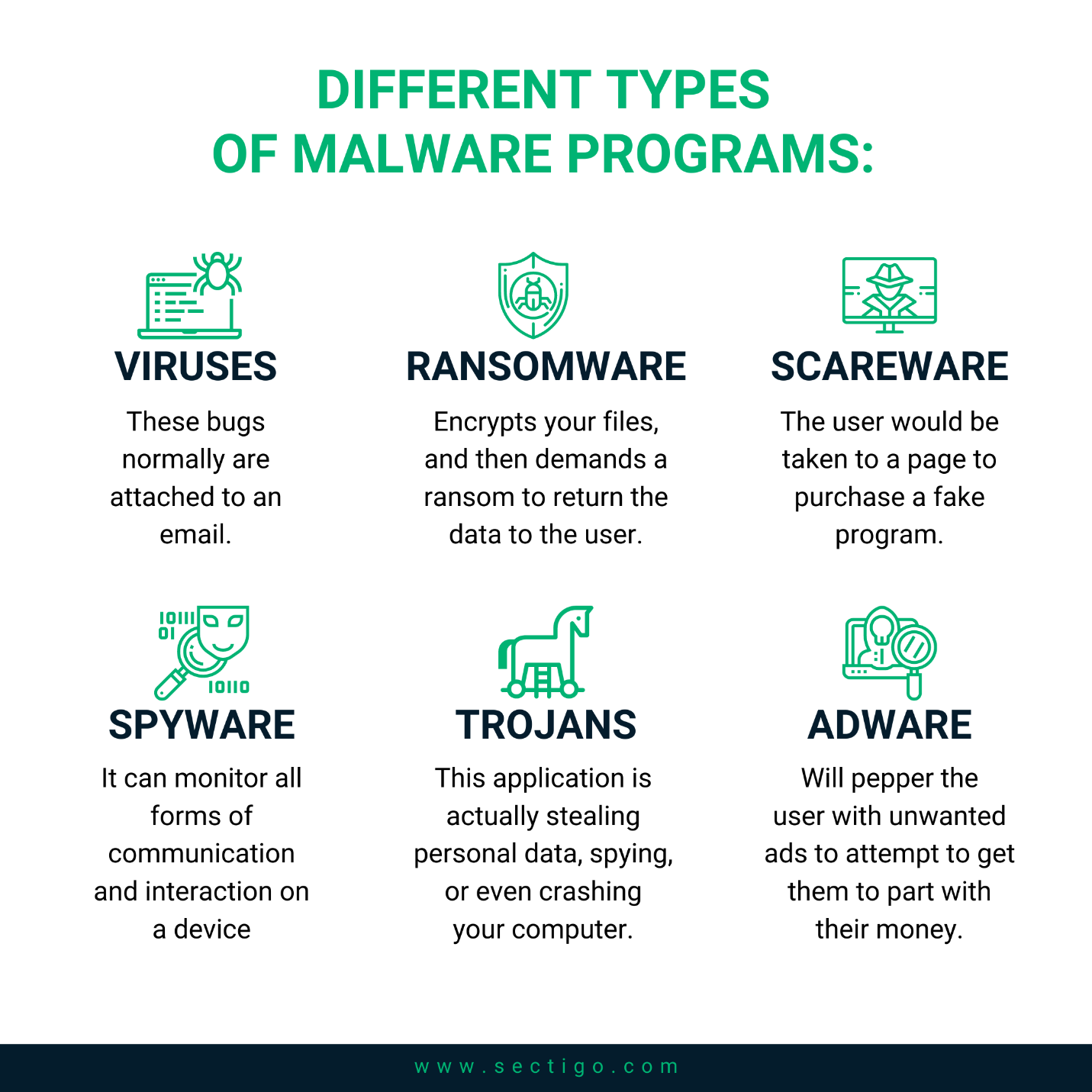
As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

* **Spear phishing**

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They’re much harder to detect and have better success rates if done skillfully.

**Malware and Types:**

**Malware** is a catch-all term for any type of malicious software designed to harm or exploit any programmable device, service or network. Such as virus, worms, trojan horse, spyware, adware, Ransomware.



**Antivirus, Mechanism and types of Detection**

**Antivirus:**

Antivirus is a kind of **software** used to **prevent**, **scan**, **detect** and **delete** **viruses** from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

**Mechanism:**

An antivirus software works by **scanning** **incoming** **files** or code that's being passed through your **network** **traffic**. Companies who build this software compile an extensive database of already known **viruses** and **malware** and teach the software how to **detect**, **flag**, and **remove** them.

**Types of detection:**

There are four major methods of virus detection in use today: **scanning**, **integrity** **checking**, **interception**, and **heuristic** **detection**. Of these, scanning and interception are very common, with the other two only common in less widely-used anti-virus packages.

**Hash types & its Applications**

A hash is a function that converts one value to another. Hashing data is a common practice in computer science and is used for several different purposes. Examples include cryptography, compression, checksum generation, and data indexing. The table may be an array, database, or other data structure.

**Types of Hashing**

There are many different types of hash algorithms such as RipeMD, Tiger, xxhash and more, but the most common type of hashing used for file integrity checks are MD5, SHA-2 and CRC32. MD5 - An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint.

**MD5** - An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint. MD5 is often used as a checksum to verify data integrity. However, due to its age, MD5 is also known to suffer from extensive hash collision vulnerabilities, but it’s still one of the most widely used algorithms in the world.

**SHA-2** – SHA-2, developed by the National Security Agency (NSA), is a cryptographic hash function. SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

**CRC32** – A cyclic redundancy checks (CRC) is an error-detecting code often used for detection of accidental changes to data. Encoding the same data string using CRC32 will always result in the same hash output, thus CRC32 is sometimes used as a hash algorithm for file integrity checks. These days, CRC32 is rarely used outside of Zip files and FTP servers.

**Applications of Hash:**

There are many other applications of hashing, including modern day cryptography hash functions. Some of these applications are listed below:

* **Message Digest**

This is an application of cryptographic Hash Functions. Cryptographic hash functions are the functions which produce an output from which reaching the input is close to impossible. This property of hash functions is called irreversibility.

* **Password Verification**

Cryptographic hash functions are very commonly used in password verification.

* **Data Structures (Programming Languages)**

Various programming languages have hash table based Data Structures. The basic idea is to create a key-value pair where key is supposed to be a unique value, whereas value can be same for different keys.

* **Compiler Operation**

The keywords of a programming language are processed differently than other identifiers. To differentiate between the keywords of a programming language (if, else, for, return etc.) and other identifiers and to successfully compile the program, the compiler stores all these keywords in a set which is implemented using a hash table.

* **Rabin-Karp Algorithm**

One of the most famous applications of hashing is the Rabin-Karp algorithm. This is basically a string-searching algorithm which uses hashing to find any one set of patterns in a string. A practical application of this algorithm is detecting plagiarism.

* **Linking File name and path together**

When moving through files on our local system, we observe two very crucial components of a file i.e. file\_name and file\_path. In order to store the correspondence between file\_name and file\_path the system uses a map (file\_name, file\_path) which is implemented using a hash table.