## AVOIDING MALWARE

Online sales and services, social networking, and the availability of information on the Internet have grown tremendously over the past decade. It's not surprising that as the Internet becomes more and more a part of our lives, we see a rise in nefarious activity.

Two years ago there were nearly 3 million unique forms of malicious code, and thousands of new ones are discovered daily. Malware is becoming more pervasive and fosters a legitimate concern that personal and financial information could be compromised. The risk of being infected is greater than ever because every single possible data communication method can be used to transmit malware. However, if we understand the origins of malware and how to avoid it, we are able to peruse the Internet with more confidence.

### What exactly is malware?

Malware is short for malicious software. Hackers use this software to disrupt computer operations, gather sensitive information, or gain unauthorized access to a computer system. Malware can also appear in the form of a script or code. The term 'Malware' is used to describe a variety of forms of hostile, intrusive, or annoying software or code.

You've probably heard of the terms "virus" and "worm". Although they do different things and cause different types of problems, they are both a kind of malware. Another kind of malware is the Trojan horse.  Let's take a closer look at these three.

### Computer virus

- A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes, most computer viruses are considered malicious.

### Worms

- Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people confuse the terms "virus" and "worm", using them both to describe any self-propagating program.

### Trojan horses

- A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A Trojan horse can be used to set up a back door in a computer system so that the intruder can gain access.

### What is the motivation behind malware?

In the early days of the Internet, viruses were written as experiments or pranks. In some cases, the perpetrator did not realize how much harm his or her creations would do.

Today, cybercriminals use malware to turn a profit. Infected computers are used to generate income in many ways, including advertising. Just as many legitimate websites generate income by displaying ads, malware can also display ads that result in payments to the cybercriminal. Infected computers are also used to gather information, such as credentials for online banking. This type of "banking" malware is one of the most sophisticated and stealthy forms of malware. The criminals can then use the private information they've stolen - like social security numbers and credit card account information - for their own malicious schemes or they can sell it to a third-party who uses it to make a profit. The damage caused can range from a minor annoyance to a catastrophic disaster.

**How could I get infected?**
Unfortunately, there are many ways to get infected; and there is no particular way to identify that your computer has been compromised. Anti-virus software might alert you that it has found a virus, but other forms of malware may go undetected.

Here are some of the ways you can get infected:

1. Email Attachments – Before opening email, ensure that attachments you receive are legitimate
2. Portable Media – any device that can store information can support malicious content
3. Visiting Malicious Websites – any legitimate website can be compromised by an attack, which in turn could leave you at risk
4. Downloading Files from Websites – including generic files, software, plug-ins, movies, audio files, as well as mobile code such as ActiveX, JavaScript, Flash etc
5. Participating in P2P File Sharing Services – peer-to-peer file sharing systems, especially when used to access illegal or infringing content
6. Instant Messaging Clients – especially if unpatched, they allow hackers to upload or download files through holes in the client software.
7. New Devices and Peripherals – although it's rare, mobile phones, digital photo frames, etc can be compromised during manufacturing if the manufacturer's system is infected.
8. Social Networking Sites – offer several situations that could put you at risk of infection
   - Social engineering attacks that trick users into harming their own environment
   - Hyperlinks leading to malicious sites or infected files
   - In-site applications that can be compromised by malicious entities
9. Social Engineering Attacks – that trick users into either giving up information or unwittingly performing tasks that result in a security breach
10. Not Following Security Guidelines and Policies – bypassing filters, using unauthorized outside storage devices, blocking software updates, using non-approve software clients, etc, increase the chance of becoming infected by malicious code

**How can I avoid becoming infected?**
The old wisdom rings true: an ounce of prevention is worth a pound of cure. There are things you can do to avoid becoming infected:

1. Keep software up to date so that attackers can't take advantage of known problems or vulnerabilities.
2. Use and maintain anti-virus software and malware software.
3. Use and maintain anti-spyware tools.
4. Install a firewall to shield your computer or network from malicious or unnecessary Internet traffic.
5. Add location-aware client firewall software on mobile devices including laptops to enforce tighter security when connected to any non-trusted network, such as a free Wi-Fi hotspot.

6. Evaluate your security settings in your software, browsers, email programs and online accounts.
7. Use strong passwords & change them periodically.
8. Disconnect your computer from the Internet when you aren't using it.
9. Maintain backups of your files on CDs or DVDs so that you have saved copies in case you get infected.
10. Follow good security practices and take appropriate precautions when using email and web browsers to reduce the risk that your actions will trigger an infection.