Computers I

## 2.4 Securing your computer when on the web

A lot of vulnerabilities exist when surfing the web and you have probably heard of them all but what do they actually mean and how do they work? In this lesson we will be covering everything you need to know about viruses and the different kinds that exist.

### 2.4.1 Malware concepts

Malware – short for malicious software is any software used to disrupt, destroy and gain access to sensitive information.

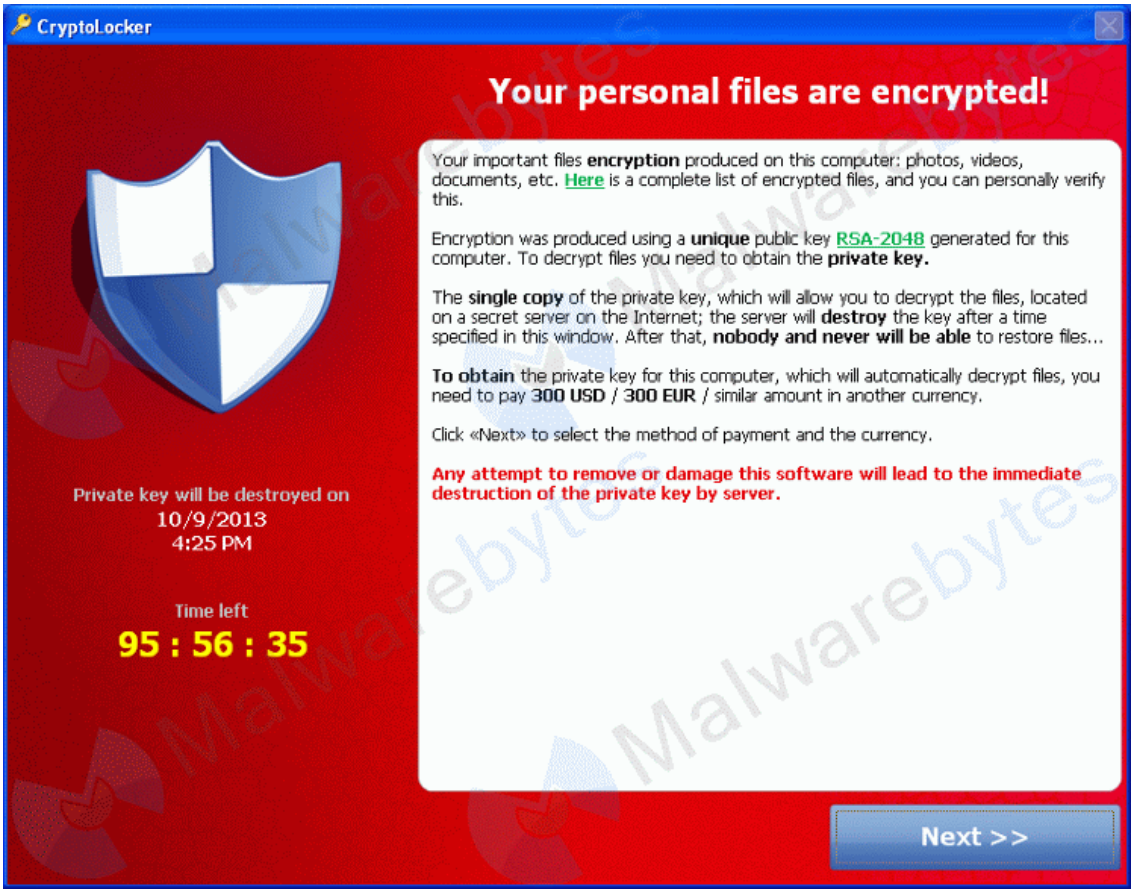
Malware encompasses different types of virus including worms and Trojans as well as ransomware, spyware, adware, and scareware.

Spyware – type of malware installed on a computer that collects information on the user without their knowledge.

Adware – malware that automatically plays, or downloads advertisements

Scamware - this includes fake popups on your computer claiming you have a virus. This is the actual virus however, and they want you to buy their “antivirus” to clean your system. In reality, your card just got stolen by the antivirus virus.

Ransomware – this malware encrypts your files and threatens to delete it within a certain amount of time unless you pay. Essentially you are held ransom.




It is easy to know if you have a virus

- Antivirus lets you know
- Strange messages appear
- Computer crashes frequently
- Strange files you do not know appear
- Computer slows down and hard drive space is reduced
- Program not working like it used to

## 2.4.2 Virus Types

What is a computer virus?

A computer virus refers to a program, which damages computer systems and destroys or erases data files.

Payload - the part of the malware that actually performs the damaging action.

Types of Viruses

- Time Bomb – performs an activity on a specific date
- Logical Bomb – performs when a certain action is performed

- Worm – fills a computer with self-replicating information without the need of human interaction, slows your system. Spread through the Internet and local area networks, can spread through e-mails, messages and chats. Uses a lot of your network resources slowing down your connection

- Boot Sector Virus – infects boot sector of computers. When the system boots, the virus is loaded into memory and destroys data in hard disk.
- Macro Virus – attach through word or excel and when opened is loaded into main memory. Macros are normally mini-programs that make tedious task simple and easy to do with a single action.

  No longer common – W97M.Melissa

- Trojan Horse – Destructive program that pretends to be software, or game that you want and can seriously harm the computer by causing data loss and theft. Do not replicate

Keylogger – associated with Trojans gather computers keystrokes to potentially determine passwords, usernames, social security numbers, and any other critical information that may have been typed in.

Modern government websites require you to click rather than type sensitive information.

Some viruses do not steal information but are still an intrusion and can show messages on your screen such as the Happy99 worm.


Other than forcing this to open, and allowing itself to be spread to other computers this worm does no other damage, and its payload is the mere message and fireworks that appear.

Ways a virus can spread

- E-mail attachments
- Shared USB
- Shared files like word that contain macros
- Direct download from the Web

## 2.4.3 Phishing

Phishing is a deception designed to steal valuable personal information.

Thieves send millions of fraud e-mail messages that appear to be from trusted web sites such as your bank or credit card company, the message attempts to get you to provide personal information.

Just like fishing scammers use the emails as bait to lure you in.

Phishing scams include official-looking logos from real organization, and other information taken from the legitimate web site to make their fraudulent emails appear to be more realistic.

The emails contain threats to terminate your account if you do not reply, alert you of false intrusion, or even attempt to reward you or give you exclusive offers.

The links to phishing scams might also resemble that of the real one to trick a distracted eye. For example Microsoft.com could be changed to micosoft.com or mircosoft.com if you do not notice the subtle change you could believe you are on the actual website.

Phishing has become increasingly popular because the technical resources needed to execute phishing attacks can be readily acquired through public and private sources. In other words, Phishing has been streamlined and automated to allow use for non-technical criminals.

Most phishing scams rely on deceiving a user into visiting a malicious web site. Just as a fish is unaware that they are in danger of being caught, people are unaware that they are being targeted and might not even be aware of the types of scams that exist.

For phishing scams to work, a person must be unaware of these policies so that they are likely to be more susceptible to scams.

Your technical knowledge is irrelevant in phishing scams.

To protect yourself from phishing, be aware of the organizational policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation.

Netflix scam

1. In this scam, an e-mail is sent to the Netflix customer and warns them that they have detected unusual activity on their account and have been forced to suspend it.
2. The email if properly formatted might even look like one from Netflix. In addition to the message, the e-mail provides a phone number, and request that you call it for customer assistance.
3. When you are connected to the fake Netflix account representative, the person tells you that a hacker has infiltrated your computer, and "forwards" your call to a Microsoft Technician.
4. This fake technician then pretends to rid your system of the intrusion while actually downloading any important files from your computer.
5. They then bill you for their services and ask that you to take a photo of your ID and credit card for "credential proof" and put it onto your computer. The reason this works on people is that the scammers follow a script just as a real technician would. If a person is not computer savvy, they will think that this person is really helping, and that the way they are doing things is standard procedure.

Erika Lehman <elehman@cincinnati.bbb.org>

# Problem with your membership

1 message

**Netflix** <azure_9251ad36410308f65951aecef2f1406d@azure.com> Thu, Aug 22, 2013 at 4:44 PM
To: elehman@cincinnati.bbb.org

NETFLIX Your Account | Help

## We are missing some information

**Dear Member,**

We are glad you are a Netflix member, but we are having trouble autherizing your MasterCard.

To fix this problem, try this:

1. Go to: Netflix/Payment
2. Enter your paymyent information again or use a different payment method.
3. Click on the “Update payment method” button.

If you have any questions, we are happy to help. Just call us anytime at 1-888-811-1933.

The Netflix Team

## Facebook scam

1. In the Facebook scams, compromised accounts send messages to people's message box pretending to be a friend of the recipient. The message claims that the sender's house is on fire and burning to the ground. There is a link in the message so that the person can see footage of the fire.
2. The message comes from a hijacked Facebook account. Those who click the link will be taken to a fake Facebook login page designed to steal their real Facebook login details.
3. If you do login on the fake page, you will then be redirected to another page that claims you need download a YouTube Player update in order to view the fire video.
4. Clicking the "update" link will install a Trojan on the computer. The Trojan will collect information from your computer and allow criminals to control the computer remotely.

## 2.4.4 Protection Methods

1. Use an antivirus software

How antivirus software works

The software examines each and every file in a computer and examines its content with the virus definitions stored in its virus dictionary.

The dictionary is a file that belongs to the antivirus software that contains the code identified as a virus.

Antivirus software also constantly monitors the activity of all the programs.

If any program tries to write data on an executable file, the antivirus flags that program and investigates it, this method helps with unknown viruses, however, it can also create a false alert and spend resources investigating non threats.

2. Do not open email attachments you were not expecting
   Guard against spam, you should be cautious of emails that ask you to confirm personal or financial information over the Internet, or make urgent requests for this information by providing you with frightening information and be cautious of the sender.

3. Never enter personal information in a pop-up screen or click on unknown links; you ever know where it is really going to take you.

4. Scan downloaded files before opening them
5. Disable Macros on Word or Excel