Computer Security

DR/ HANAN HAMED
LECTURE 1

The Internet = A World of Opportunities

A myriad of information is at your fingertips

- A way to communicate with colleagues, friends, and family
- Access to information and entertainment
- A means to learn, meet people, and explore

Online Security vs Online Safety

- **Security: We must secure our computers with technology in the same way that we secure the doors to our homes.**
- **Safety: We must act in ways that help protect us against the risks that come with Internet use.**

Primary Online Risks and Threats

To Computers

(Security)

- Viruses
- Worms
- Trojans
- Spyware
- Adware

To Personal Information
(Safety)

- Online fraud and phishing
- Hoaxes
- Identity theft
- Spam

Introduction to Computer Security

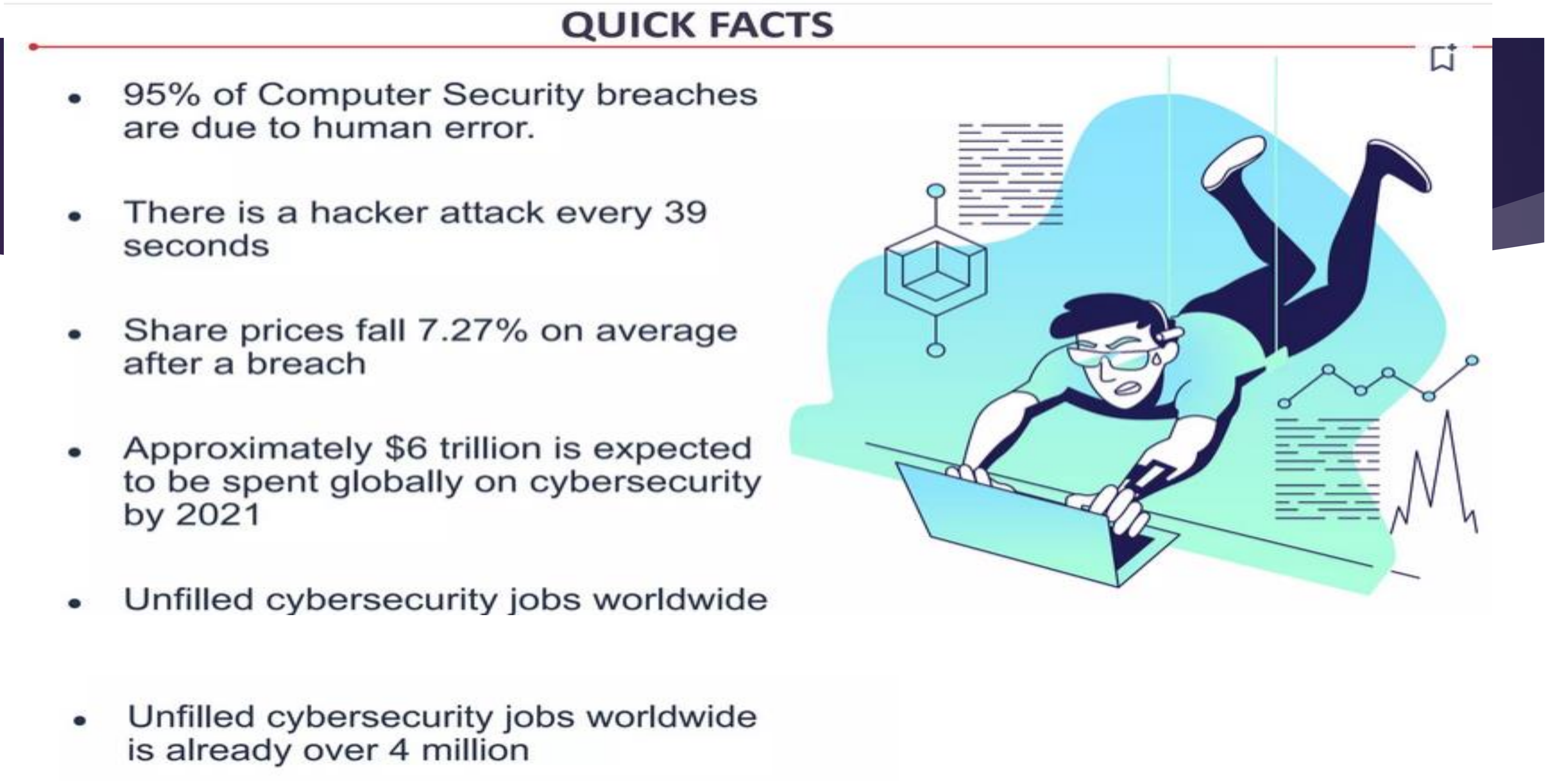
- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use.

- It is the process of preventing and detecting unauthorized use of your computer system.

- Computer Security mainly focuses on three factors:
  I. Security Attacks
  II. Security Services
  III. Security Mechanisms

Why is Computer Security Important?

- Cyber Crime is on the rise
- Damage is Significant
- Cyber Security builds trust
- Our identities protect our data
- Every organization has vulnerabilities.



QUICK FACTS

- 95% of Computer Security breaches are due to human error.
- There is a hacker attack every 39 seconds
- Share prices fall 7.27% on average after a breach
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
- Unfilled cybersecurity jobs worldwide
- Unfilled cybersecurity jobs worldwide is already over 4 million

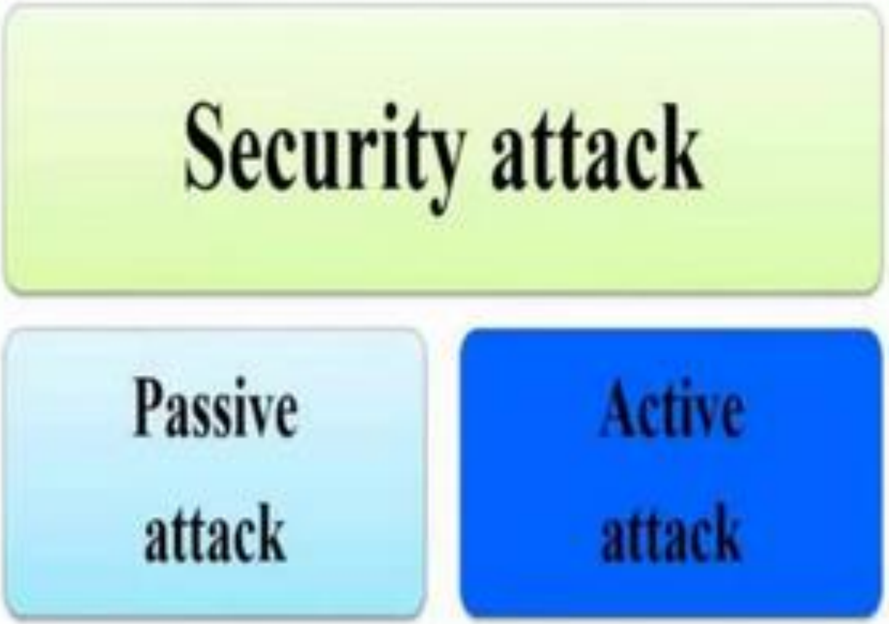
Security threat and security attack

- Threat is a possible danger that might exploit vulnerability. The actions that cause it to occur are the security attacks.
- A security attack may be a passive attack or an active attack.

➢ The aim of a passive attack is to get information from the system but it does not affect the system resources. Passive attacks are difficult to detect but can be prevented.

➢ An active attack tries to alter the system resources or affect its operations. Active attack may modify the data or create a false data. Active attacks are difficult to prevent.

- Security attacks divided into two categories:



Security attack

Passive attack

Active attack

Security Attacks on Users, Computer hardware and Computer Software

- Attacks on users could be to the identity user and to the privacy of user. Identity attacks result in someone else acting on your behalf by using personal information like password, PIN number in an ATM, credit card number, social security number etc. Attacks on the privacy of user involve tracking of users habits and actions—the website user visits, the buying habit of the user etc. Cookies and spam mails are used for attacking the privacy of users.
- Attacks on computer hardware could be due to a natural calamity like floods or earthquakes; due to power related problems like power fluctuations, etc or by destructive actions of a burglar.
- Software attacks harm the data stored in the computer. Software attacks may be due to malicious software, or, due to hacking. Malicious software or malware is a software code included into the system with a purpose to harm the system. Hacking is intruding into another computer or network to perform an illegal act.

This chapter will discuss the malicious software and hacking in detail.

Malicious Software

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared

A wide variety of malware types exist:-

1. Computer Viruses
2. Worms
3. Trojan Horses
4. Ransom ware
5. Java scripts and Java applets
6. Spyware, etc.

Virus

- A computer virus is a computer program that, when executed, replicates itself by modifying other computer programs
- It can attach itself to other healthy programs.
- It is difficult to trace a virus after it has spread across a network.
- Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links.
- Computer viruses cause billions of dollars' worth of economic damage each year.
- If a virus has entered in the system then there might be frequent pop-up windows, Frequent crashes, Unusually slow computer performance, Unknown programs that start up when you turn on your computer, Unusual activities like password changes.
- Examples of virus:- Melissa, I Love You.

Worms

- A computer worm is a type of malware that spreads copies of itself from computer to computer without any human interaction.
- Computer worms could arrive as attachments in spam emails or instant messages (IMs).
- When computer is infected with worms then it starts to take up free space of your hard drive, programs might crash, your files may be replaced or deleted.
- A worm is however different from a virus. A worm does not modify a program like a virus.
- Examples of worms:- Code Red, Nimda

Trojan Horse

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software.

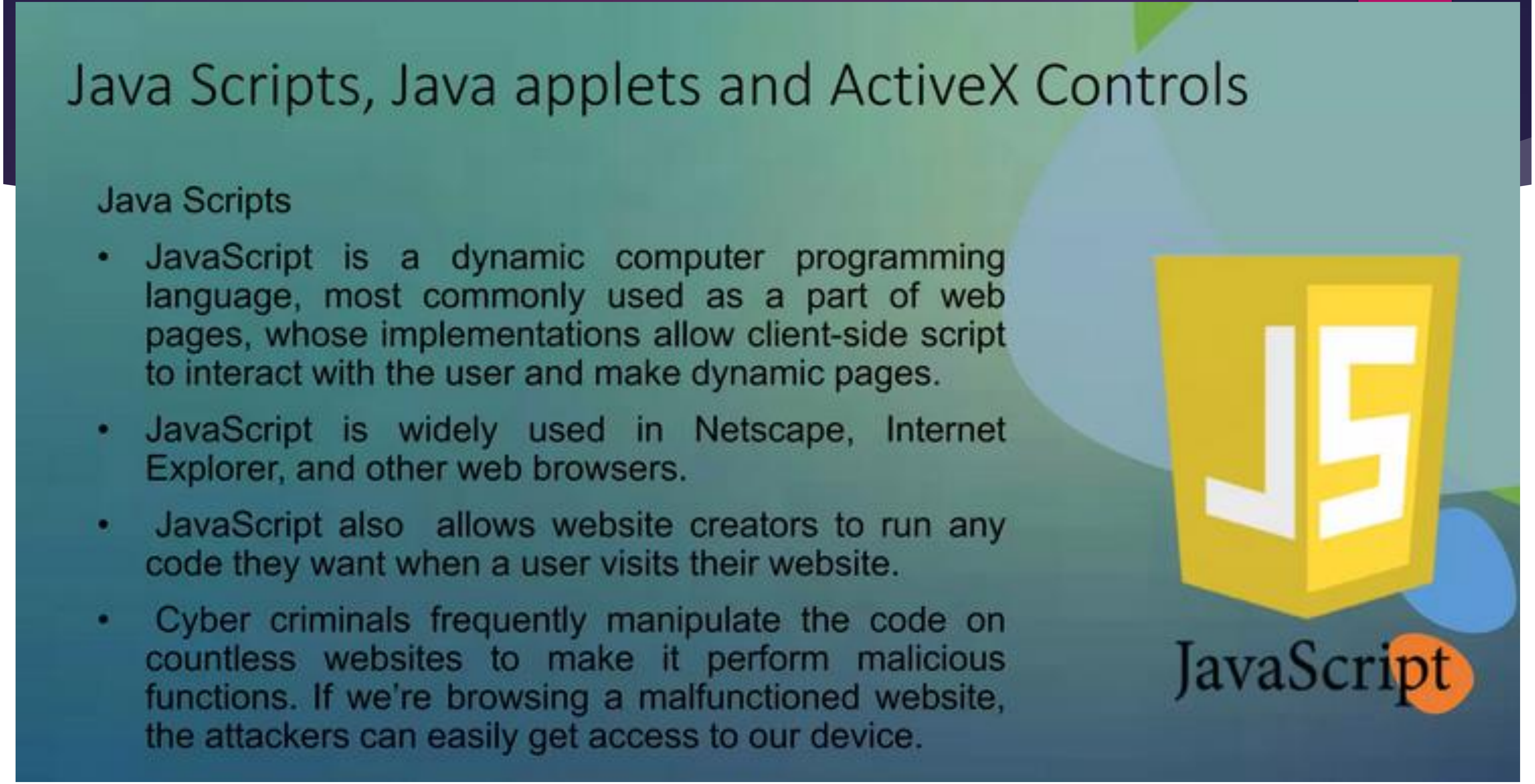
The term “Trojan” derives from the ancient Greek story about the deceptive Trojan horse which led to the fall of the city of Troy.

A Trojan must be executed by its victim to do its work.

Trojan horses contain programs that corrupt the data or damage the files, corrupt software applications.

Trojan horse does not replicate themselves like viruses.

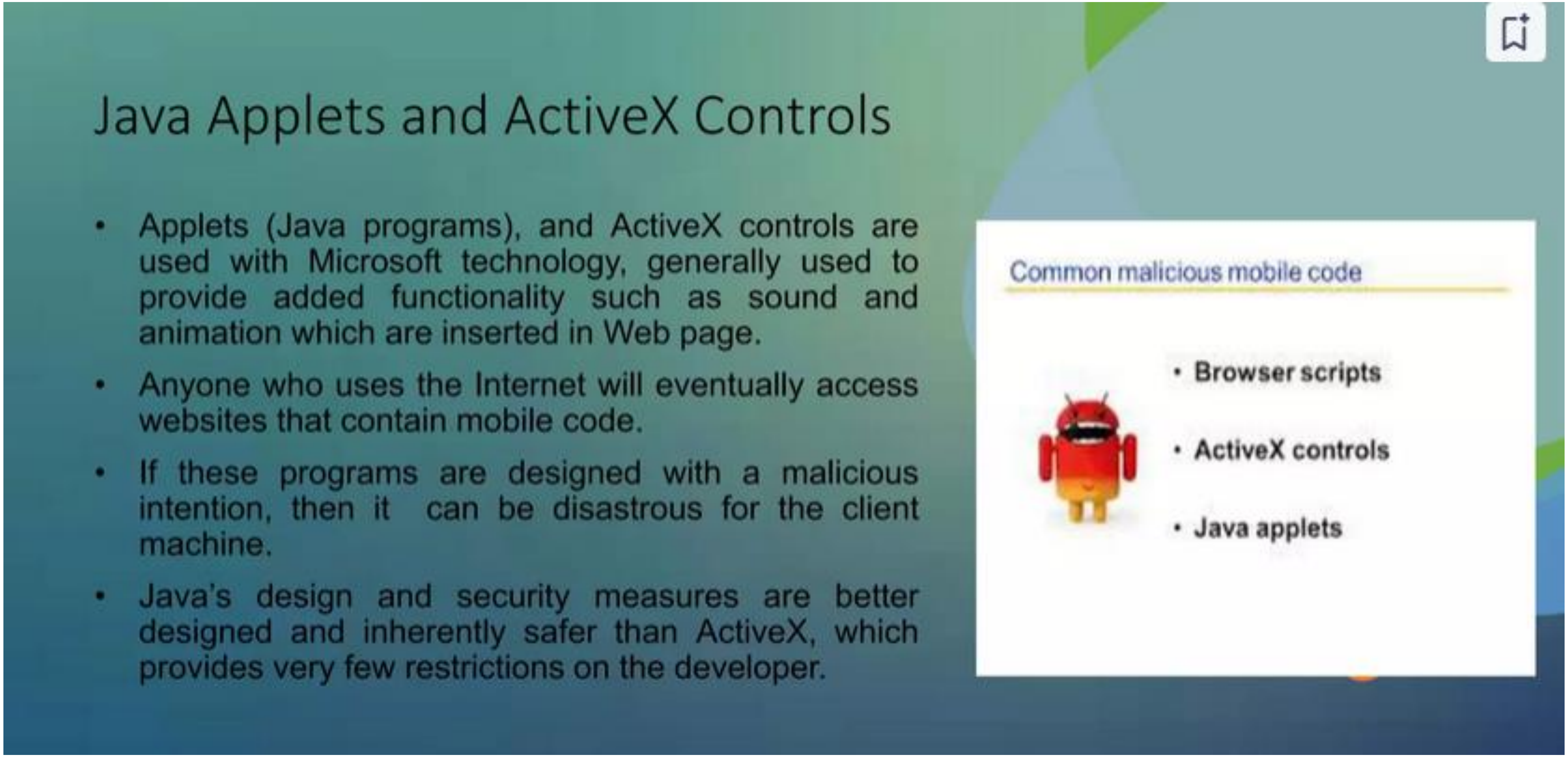
If your computer is breached by Trojan malware then, computer will start frequent crashing, redirected to unfamiliar websites when browsing online, increase in pop-ups.



Java Scripts, Java applets and ActiveX Controls

Java Scripts

- JavaScript is a dynamic computer programming language, most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages.
- JavaScript is widely used in Netscape, Internet Explorer, and other web browsers.
- JavaScript also allows website creators to run any code they want when a user visits their website.
- Cyber criminals frequently manipulate the code on countless websites to make it perform malicious functions. If we're browsing a malfunctioned website, the attackers can easily get access to our device.

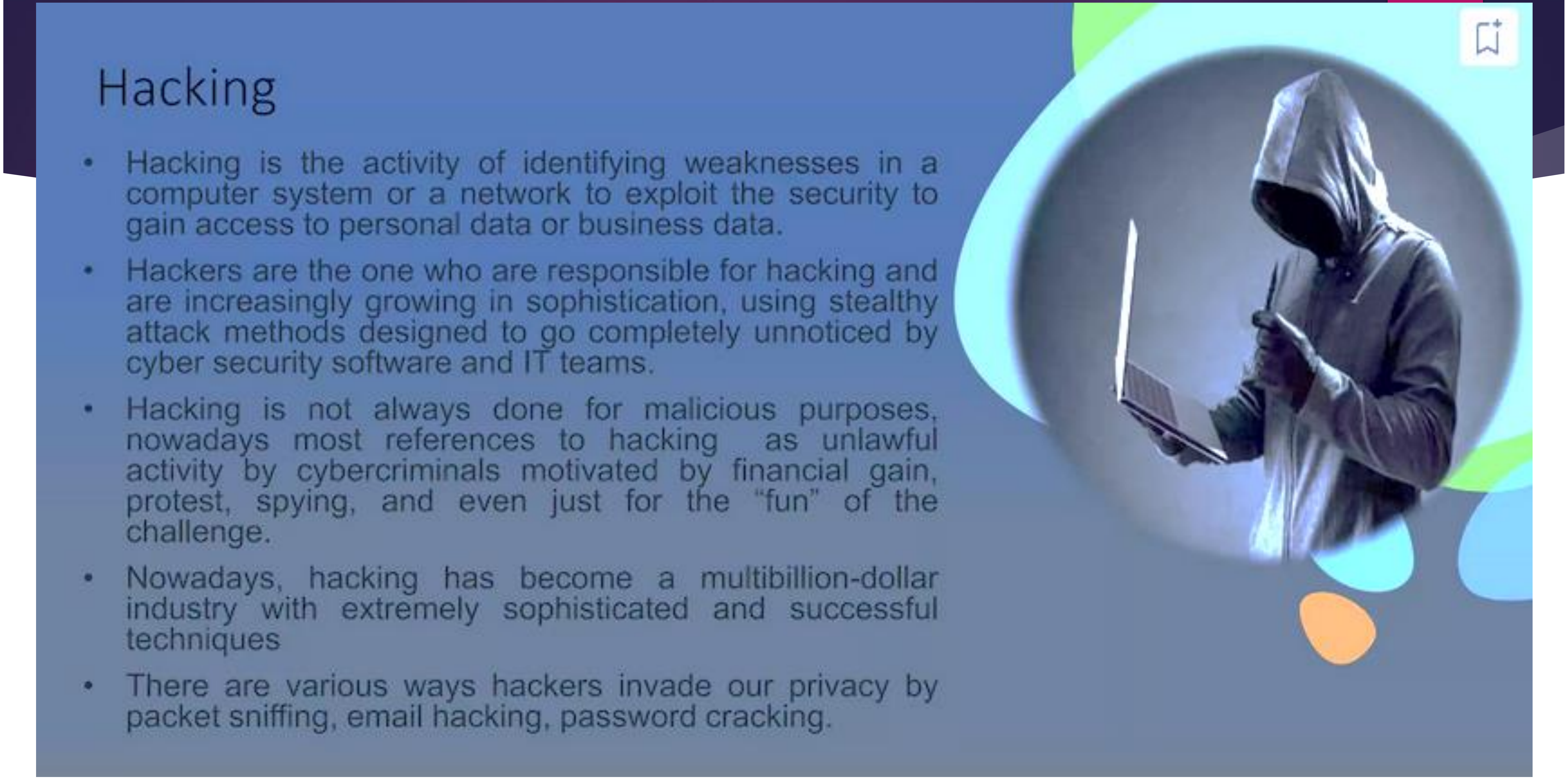


Java Applets and ActiveX Controls

- Applets (Java programs), and ActiveX controls are used with Microsoft technology, generally used to provide added functionality such as sound and animation which are inserted in Web page.
- Anyone who uses the Internet will eventually access websites that contain mobile code.
- If these programs are designed with a malicious intention, then it can be disastrous for the client machine.
- Java's design and security measures are better designed and inherently safer than ActiveX, which provides very few restrictions on the developer.

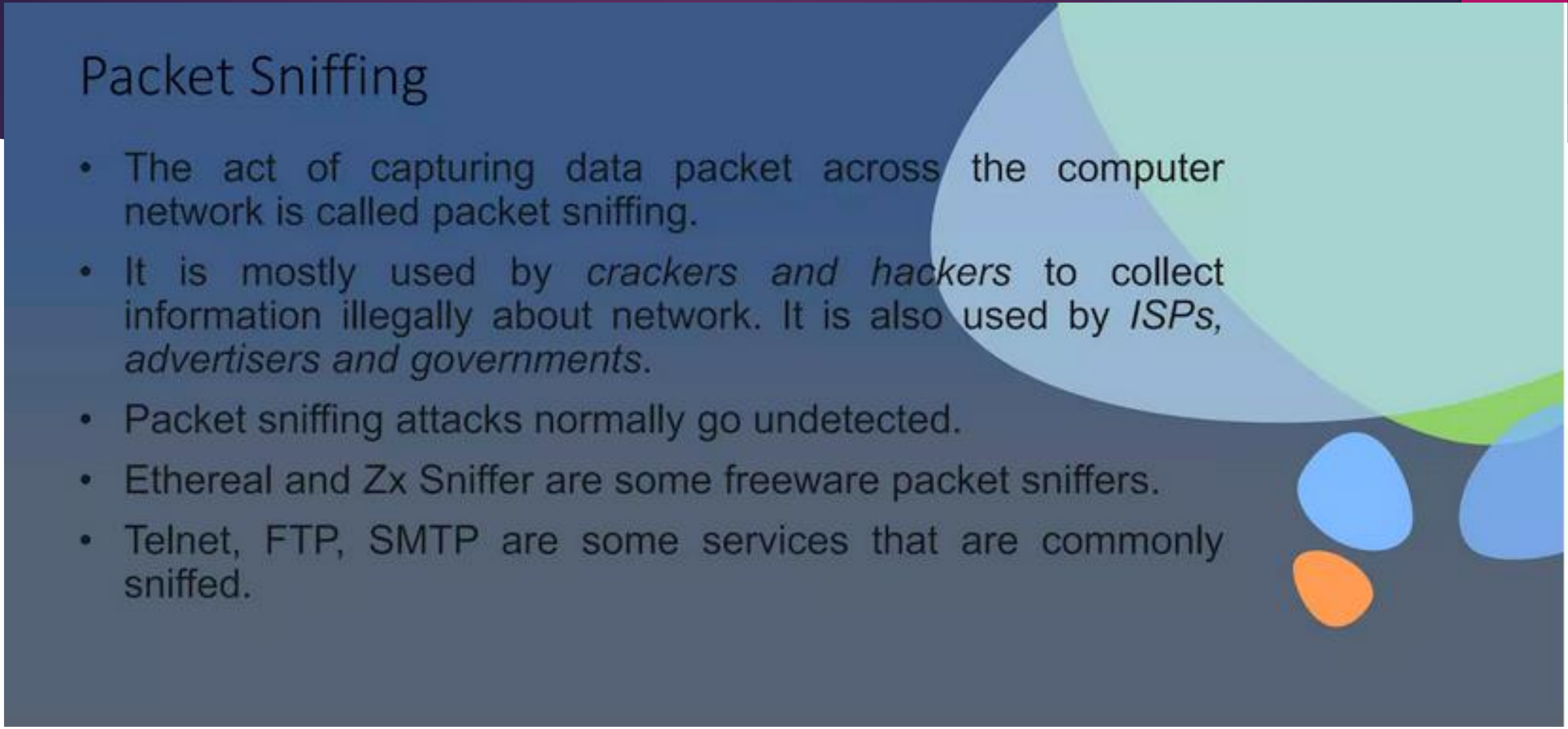
Common malicious mobile code

- Browser scripts
- ActiveX controls
- Java applets



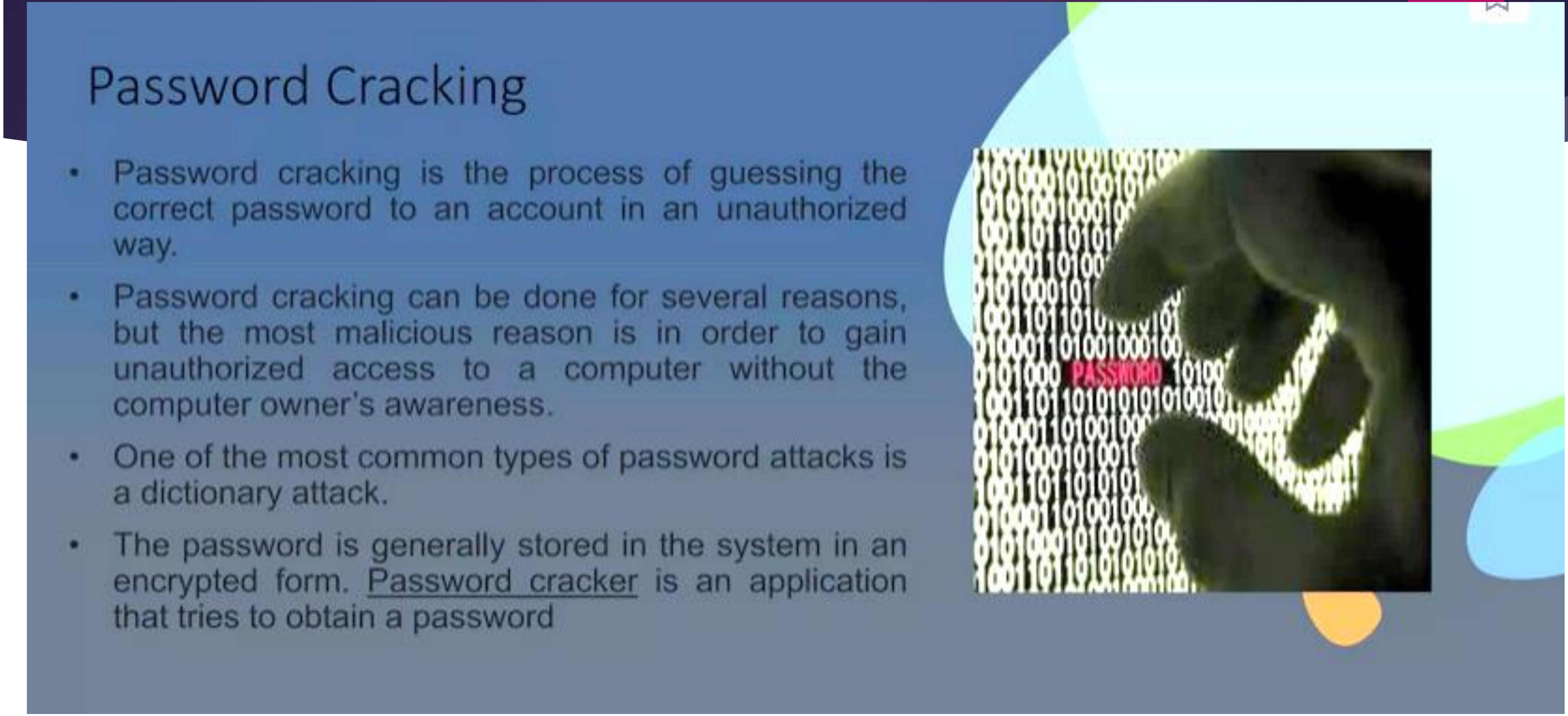
Hacking

- Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data.
- Hackers are the one who are responsible for hacking and are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cyber security software and IT teams.
- Hacking is not always done for malicious purposes, nowadays most references to hacking as unlawful activity by cybercriminals motivated by financial gain, protest, spying, and even just for the “fun” of the challenge.
- Nowadays, hacking has become a multibillion-dollar industry with extremely sophisticated and successful techniques
- There are various ways hackers invade our privacy by packet sniffing, email hacking, password cracking.



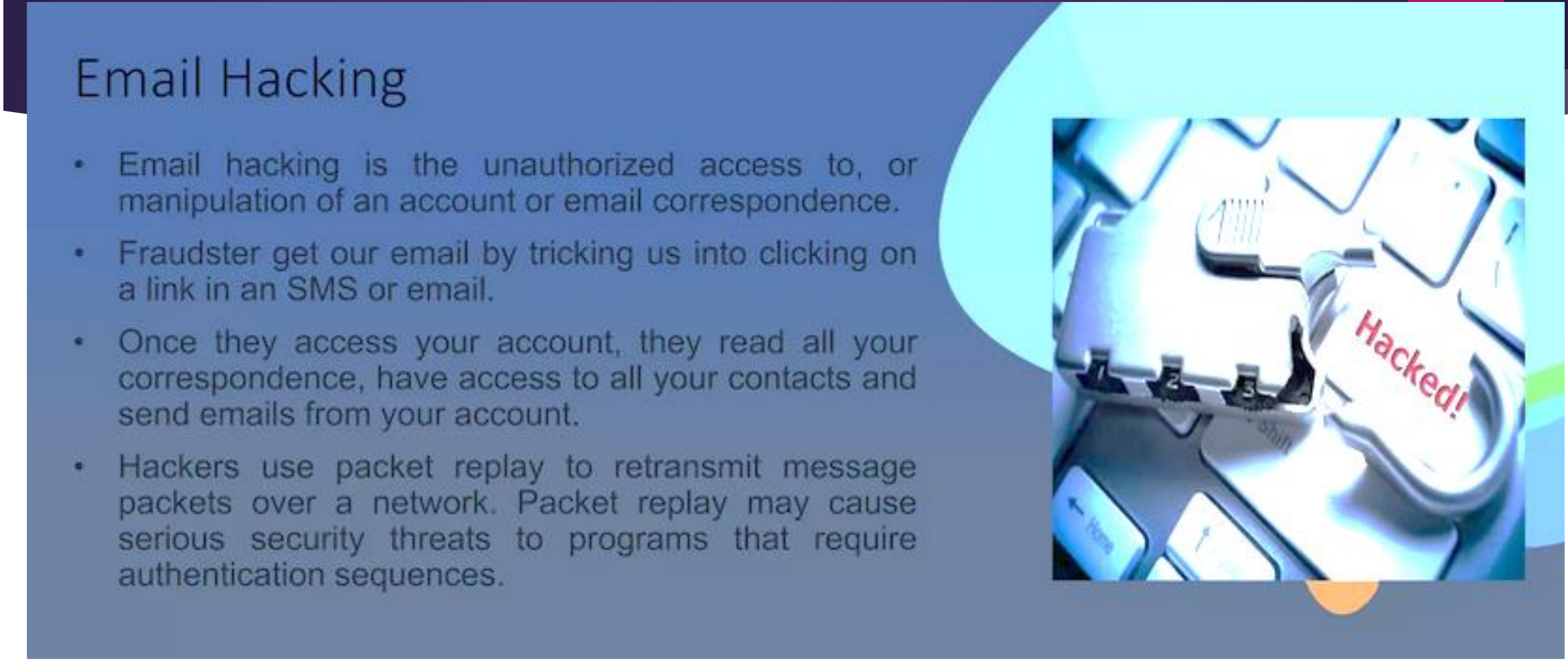
Packet Sniffing

- The act of capturing data packet across the computer network is called packet sniffing.
- It is mostly used by *crackers and hackers* to collect information illegally about network. It is also used by *ISPs, advertisers and governments*.
- Packet sniffing attacks normally go undetected.
- Ethereal and Zx Sniffer are some freeware packet sniffers.
- Telnet, FTP, SMTP are some services that are commonly sniffed.



Password Cracking

- Password cracking is the process of guessing the correct password to an account in an unauthorized way.
- Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness.
- One of the most common types of password attacks is a dictionary attack.
- The password is generally stored in the system in an encrypted form. Password cracker is an application that tries to obtain a password



Email Hacking

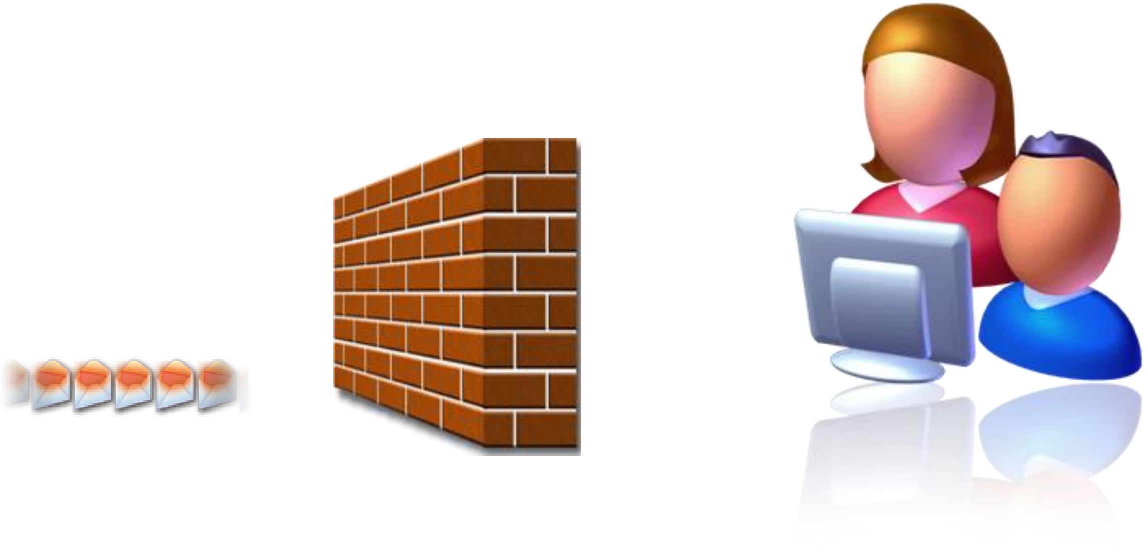
- Email hacking is the unauthorized access to, or manipulation of an account or email correspondence.
- Fraudster get our email by tricking us into clicking on a link in an SMS or email.
- Once they access your account, they read all your correspondence, have access to all your contacts and send emails from your account.
- Hackers use packet replay to retransmit message packets over a network. Packet replay may cause serious security threats to programs that require authentication sequences.

Four Steps to Help Protect Your Computer

1. Turn on Windows Internet firewall
2. Use Microsoft Update to keep Windows up-to-date automatically
3. Install and maintain antivirus software
4. Install and maintain antispyware software

Turn on Windows Internet Firewall

- The firewall helps create a protective barrier between your computer and the internet
- Some antivirus programs also come with a firewall



Use Automatic Updates to Keep Software Up-to-date

- Install all updates as soon as they are available
- Automatic updates provide the best protection

Also keep Java, Flash, and other add-on programs up to date

- These programs will prompt you when updates are available
- Always install as soon as possible

Install and Maintain Antivirus Software

- Antivirus software helps to detect and remove computer viruses before they can cause damage.
- For antivirus software to be effective, you must keep it up-to-date.

Don’t let it expire

Install and Maintain Antispyware Software

- Use antispyware software, such as Malware Bytes, so unknown software cannot track your online activity and potentially steal your information.
- Many antivirus programs now include antispyware

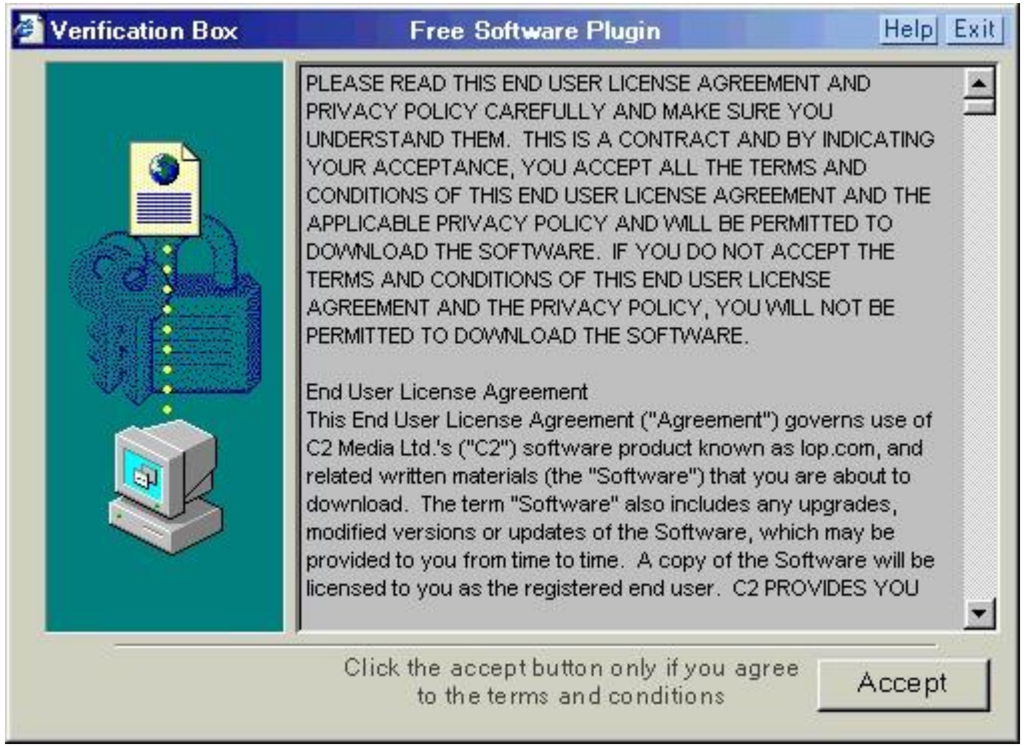
Other Ways to Help Protect Your Computer

- Back up your files regularly
- Read Web site privacy statements
- Close pop-ups using Alt+F4
- Think before you click

Back up Your Files

- make sure to store important information on network drives
- Save to CD/DVD, a USB drive, or other external source
- Use a Web-based backup service such as http://www.onedrive.com

Read Privacy Statements



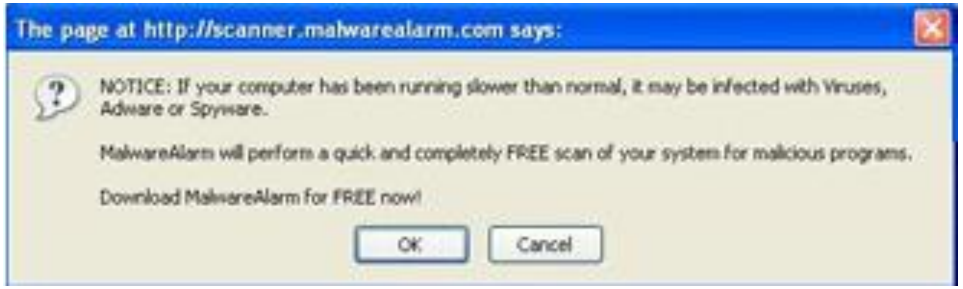
PLEASE READ THIS END USER LICENSE AGREEMENT AND PRIVACY POLICY CAREFULLY AND MAKE SURE YOU UNDERSTAND THEM. THIS IS A CONTRACT AND BY INDICATING YOUR ACCEPTANCE, YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT AND THE APPLICABLE PRIVACY POLICY AND WILL BE PERMITTED TO DOWNLOAD THE SOFTWARE. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THIS END USER LICENSE AGREEMENT AND THE PRIVACY POLICY, YOU WILL NOT BE PERMITTED TO DOWNLOAD THE SOFTWARE.

End User License Agreement
This End User License Agreement ("Agreement") governs use of C2 Media Ltd.'s ("C2") software product known as lop.com, and related written materials (the "Software") that you are about to download. The term "Software" also includes any upgrades, modified versions or updates of the Software, which may be provided to you from time to time. A copy of the Software will be licensed to you as the registered end user. C2 PROVIDES YOU

Click the accept button only if you agree to the terms and conditions

- Understand what you are getting before you agree to download or share your personal information
- Read End User License Agreements (EULA’s) before clicking “Agree” or “Accept”

Use the Alt+F4 to Close Pop-ups



The page at http://scanner.malwarealarm.com says:

NOTICE: If your computer has been running slower than normal, it may be infected with Viruses, Adware or Spyware.

MalwareAlarm will perform a quick and completely FREE scan of your system for malicious programs.

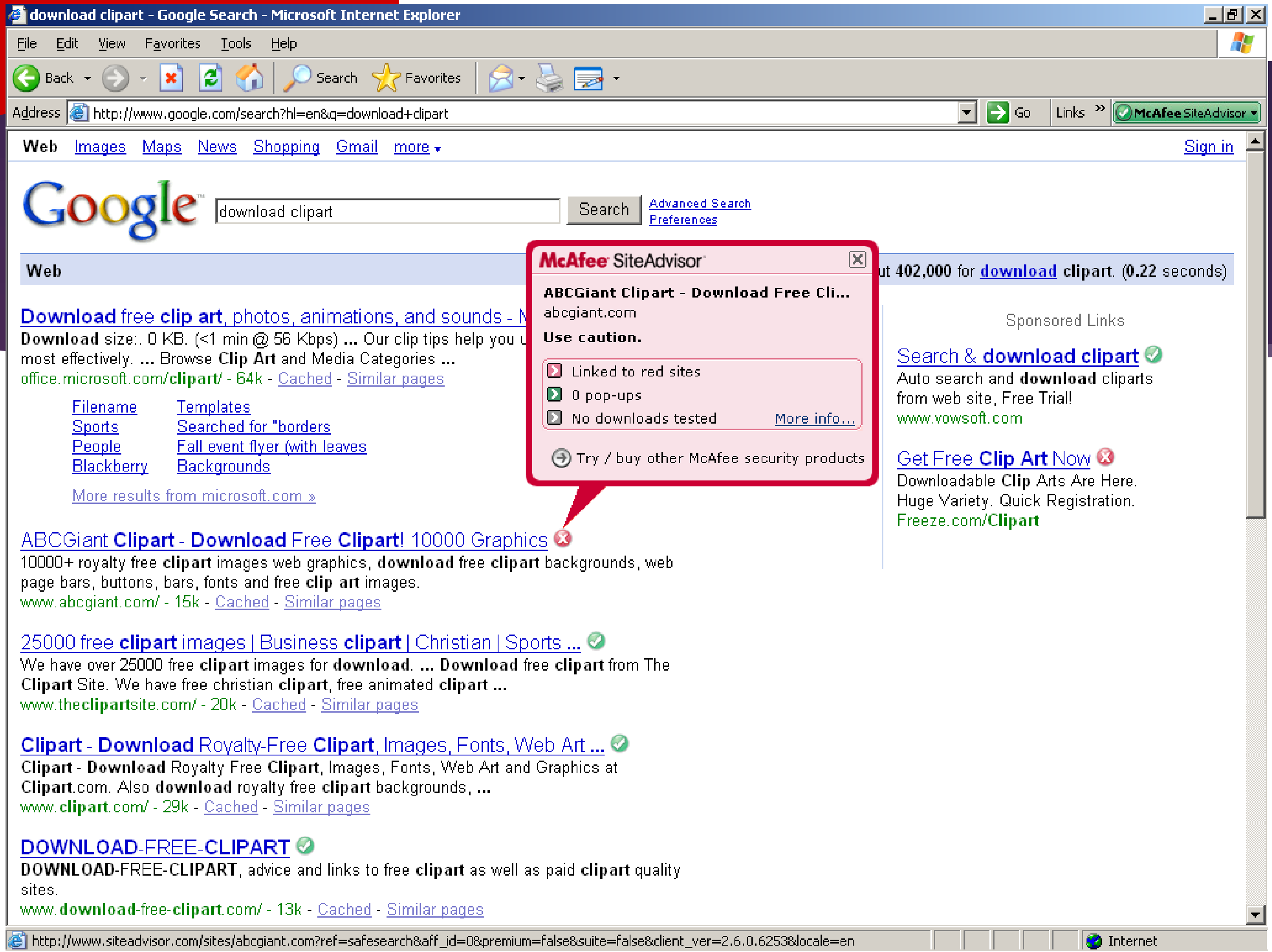
Download MalwareAlarm for FREE now!

Always press Alt+F4 on your keyboard to close pop-ups

- Never click "yes," "accept," or even "cancel" or "abort" because it could be a trick that installs software on your computer.

Think Before You Click

- Be cautious with e-mail attachments and links
- Only download files from Web sites you trust
- Use a web site advisor program such as McAfee Site Advisor


download clipart - Google Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/search?hl=en&q=download+clipart
Go Links McAfee SiteAdvisor
Web Images Maps News Shopping Gmail more
Sign in
Google
download clipart
Search
Advanced Search
Preferences
Internet

Web

...ut 402,000 for **download** clipart. (0.22 seconds)

McAfee SiteAdvisor

ABCGiant Clipart - Download Free Cli...
abcgiant.com
Use caution.

☒ Linked to red sites
☒ 0 pop-ups
☒ No downloads tested More info...

Try / buy other McAfee security products

Download free **clip art**, photos, animations, and sounds - M...
Download size:. 0 KB. (<1 min @ 56 Kbps) ... Our clip tips help you u... most effectively. ... Browse **Clip Art** and Media Categories ...
office.microsoft.com/**clipart**/ - 64k - Cached - Similar pages

Filename	Templates
Sports	Searched for "borders
People	Fall event flyer (with leaves
Blackberry	Backgrounds

More results from microsoft.com »

ABCGiant **Clipart** - **Download** Free **Clipart**! 10000 Graphics
10000+ royalty free **clipart** images web graphics, **download** free **clipart** backgrounds, web page bars, buttons, bars, fonts and free **clip art** images.
www.abcgiant.com/ - 15k - Cached - Similar pages

25000 free **clipart** images | Business **clipart** | Christian | Sports ...
We have over 25000 free **clipart** images for **download**. ... **Download** free **clipart** from The **Clipart** Site. We have free christian **clipart**, free animated **clipart** ...
www.the**clipart**site.com/ - 20k - Cached - Similar pages

Clipart - **Download** Royalty-Free **Clipart**, Images, Fonts, Web Art ...
Clipart - **Download** Royalty Free **Clipart**, Images, Fonts, Web Art and Graphics at **Clipart**.com. Also **download** royalty free **clipart** backgrounds, ...
www.**clipart**.com/ - 29k - Cached - Similar pages

DOWNLOAD-FREE-CLIPART
DOWNLOAD-FREE-CLIPART, advice and links to free **clipart** as well as paid **clipart** quality sites.
www.**download**-free-**clipart**.com/ - 13k - Cached - Similar pages

Sponsored Links

Search & **download clipart**
Auto search and **download** cliparts from web site, Free Trial!
www.vowsoft.com

Get Free **Clip Art** Now
Downloadable **Clip** Arts Are Here. Huge Variety. Quick Registration.
Freeze.com/**Clipart**

http://www.siteadvisor.com/sites/abcgiant.com?ref=safesearch&aff_id=0&premium=false&suite=false&client_ver=2.6.0.6253&locale=en

Download free from ▶

http://www.siteadvisor.com

Primary Threats to Personal Online Safety

Phishing

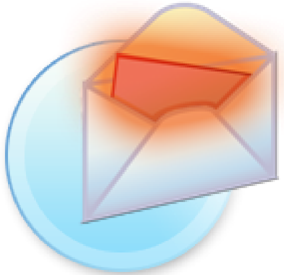
E-mail sent by online criminals to trick you into going to fake Web sites and revealing personal information

Identity Theft

A crime where con artists get your personal information and access your cash and/or credit

Hoaxes

E-mail sent by online criminals to trick you into giving them money



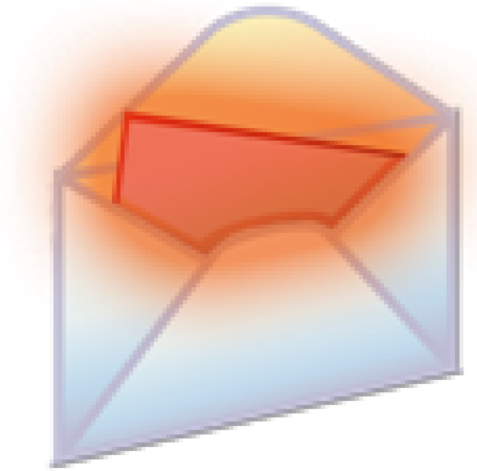
Spam

Unwanted e-mail, instant messages, and other online communication

Three Steps to Help Protect Your Personal Information

1. **Practice** Internet behavior that lowers your risk
2. **Manage** your personal information carefully
3. **Use** technology to reduce nuisances, and raise the alarm when appropriate

Practice Internet Behaviors that Help Reduce Your Risk



- Look for ways to reduce spam
- Be on the lookout for online scams
- Use strong passwords

Ways to Reduce Spam

- You usually can tell a spam message by it’s title, so never open those messages, delete them right away!
- Never reply to a spam message or click their “remove me” links- it will generate MORE spam
- Create a free online email account (Yahoo, MSN, Gmail) and use that account for offers online

Avoid Online Scams

Seven telltale signs of a scam:

1. You don't know the person and they are not with a reputable company.
2. You are promised untold sums of money for little or no effort on your part.
3. You are asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process.
4. You are asked to provide your bank account number or other personal financial information, even if the sender offers to deposit money into it.
5. The request contains a sense of urgency.
6. The person repeatedly requests confidentiality.
7. The person offers to send you photocopies of government certificates, banking information, or other "evidence" that their activity is legitimate (these are fake).

Use Strong Passwords

How secure is your password???

http://www.microsoft.com/protect/yourself/password/checker.mspx

"Rumpelstiltslkin is too long for a password!"

Choosing secure passwords

Do Not:

- Use your name or your Username in any form
- Use your spouse's, child's or pet’s name
- Use other information easily obtained about you (License plate, telephone, or social security numbers, brand of your automobile, street address, etc.)
- Use words found in dictionaries

Choosing secure passwords

Do:

- Use a password with mixed-case alphabetic characters
- Use a password with non-alphabetic characters (e.g., digits or punctuation)
- Use a password that is easy to remember, so you don't have to write it down
- Try using a the first letter of each word in a long phrase, then substitute caps and symbols

Choosing a secure password

Examples of Bad Passwords:

- johnd, dnhoj, johndjohnd, JOHND, ABC123D, StarWars, 0123456789, xxx999, mydogRover, truck, ILoveTom

Examples of Good Passwords:

- WAter5, Si11ymE, Ez24get, Mt4bwY

FSU Password Requirements

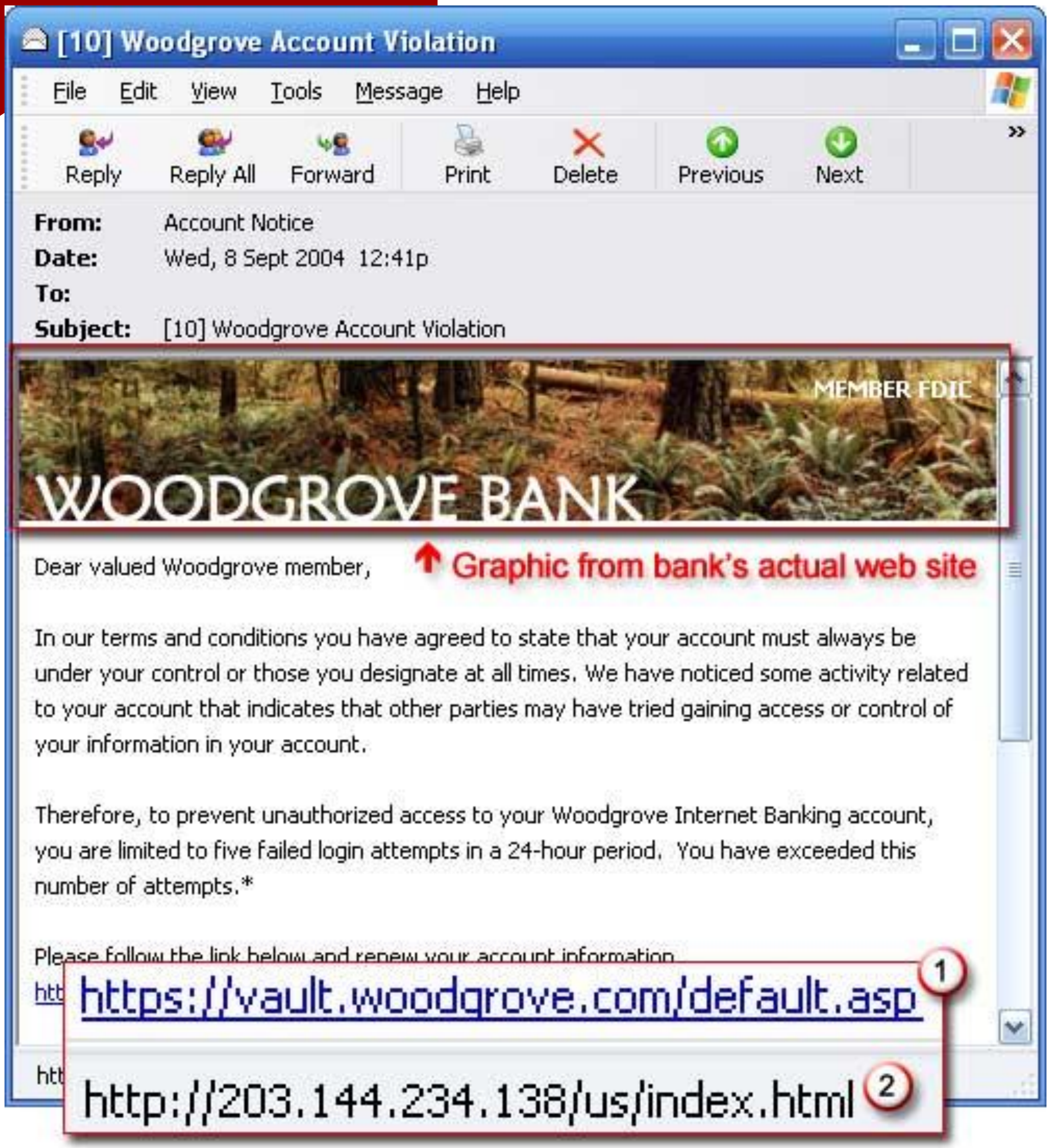
- Password must be a minimum length of eight characters
- Password cannot contain all or part of your User name
- At least 10 unique passwords must be used before a password can be reused
- Password must contain a combination of three of the following categories: uppercase characters (A thru Z), lowercase characters (a thru z), numeric (1 thru 9), and non-alphabetic characters (!,@,#,$,%, etc.)

Manage Personal Information Carefully

- Do not share personal information in e-mail or instant messages
- Use only secure and trusted Web sites
- Make sure you are where you think you are: Web sites can be faked
- Avoid financial transactions over unsecured wireless networks
- When in public, stay private

Have you been Phished?

- Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.
- Phishers send an email to get you to go to a web site where you are fooled into exposing your passwords or even banking information so they can take the money in your account.



From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation

Graphic from bank's actual web site

Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

htt https://vault.woodgrove.com/default.asp

htt http://203.144.234.138/us/index.html

- Sample Phishing email from a bank

From: Webmaster [mailto:shawws@guilford.edu]
Sent: Thursday, March 10, 2011 5:25 AM
Subject: User Quarantine Release Notification

Hello,

We are carrying out a routine quarantine exercise . we have started our yearly server (inactive email-accounts / spam protecting etc) clean-up process to enable service upgrade/migration efficiency. Please be informed that your account usage will be fully restricted if you do not adhere to this notice.

You are to provide your account details for immediate Quarantine by clicking on your reply button to respond as follows (This will confirm your account login/usage
Frequency / account continuation potentials):

*Username:
*Password:
*Alternate Email:

All IT Service utilities will not be altered during this period, This will not affect the operation of your IT service systems or the manner in which you currently login to your account. Account access and usage will be disabled if you fail to comply as required.

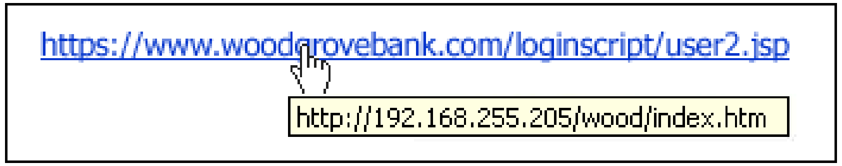
Help Desk
Information Technology
© 2011 All rights reserved

- Sample Phishing email sent to FSU users

Ways to Tell that an Email Message is Fraudulent

Phrases to look for:

- "Verify your account."
- "If you don't respond within 48 hours, your account will be closed."
- "Dear Valued Customer."
- "Click the link below to gain access to your account."



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm

How to Protect Yourself

- Never follow links or call phone numbers listed in an email. Type the company’s URL directly in a new browser window, or call the number listed on your statement.
- When in doubt, delete. Delete any email you have doubts about, especially one that requests you to give up your personal, private information.
- If you feel the email looks suspicious, report the email to the 'real' company.

How to shop online more safely

Before you select a store:

- Do a background check. Look for a physical address (not a Post Office box), request a catalog by mail, or call and talk to a company representative.
- Explore the Web site for third-party seals of approval such as:

  BBBOnline (Better Business Bureau Online)

  or

  TRUSTe

- Find out what other shoppers have to say (Epinions or Bizrate)
- Review their shipping methods and policies

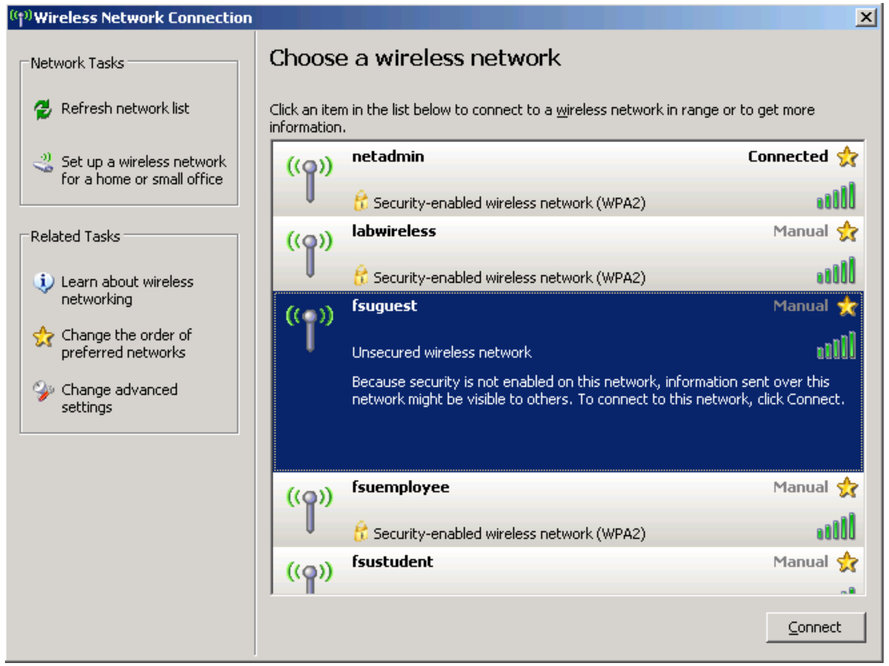
Before You Enter a Credit Card Num

- The company should only require personal information that's necessary to complete the purchase (you will probably enter your credit card number, address, and telephone number).
- The Web site should use secure technology. When you get to the screen where you enter your credit card number or other personal information, make sure that the Web address begins with *https* (for example, https://www.tailspintoys.com) and check to see if a tiny locked padlock appears next to the URL.

Use Public Wireless Networks More Safely

If a wireless network is unsecured:

- Use a firewall
- Don't type in credit card numbers or passwords
- Turn off your wireless network when you're not using it



Wireless Network Connection

Network Tasks

Refresh network list

Set up a wireless network for a home or small office

Related Tasks

Learn about wireless networking

Change the order of preferred networks

Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

netadmin — Connected — Security-enabled wireless network (WPA2)

labwireless — Manual — Security-enabled wireless network (WPA2)

fsuguest — Manual — Unsecured wireless network

Because security is not enabled on this network, information sent over this network might be visible to others. To connect to this network, click Connect.

fsuemployee — Manual — Security-enabled wireless network (WPA2)

fsustudent — Manual

Check your Social Network settings

- Do you know what other people can see on your Facebook or Twitter page?
- Be careful what you post
- “If you can’t say something nice, don’t say nothing at all”
- Google yourself!

Secure Your Wireless at Home

- Wireless networks often extend more than 300 feet from your wireless router.
- It's one thing to let a neighbor borrow your lawn mower, but you should think twice about allowing anyone to access your home network!

- Out of the box, many wireless routers are completely unsecured

Tips for Wireless Home Network Security

- Change Default Administrator Passwords (and Usernames)
- Turn on (Compatible) WPA / WPA2 Encryption
- Change the Default SSID
- Disable SSID Broadcast
- Enable Firewalls On Each Computer and the Router
- Position the Router or Access Point Safely
- Turn Off the Network During Extended Periods of Non-Use
- Change passwords and WPA / WPA2 keys regularly