Online Security

Ifeoma Adaji

Learning objectives

- Define what online/cyber security is
- List and explain types of online security threats and ways to prevent them
- Explain what hacking is and the common types of hackers
- Explain who is responsible for online security
- Describe cyber security laws that exist in US and Canada

Online security

- Rules, actions and processes that happen to ensure safety on the internet
- Tactics for protecting activities and transactions carried out online
- Security is essential because:
  - Many of our daily activities are carried out online – tons of data and sensitive information is constantly being shared online
  - High risk of intrusion by hackers and cybercriminals

Types of online security threats

- Malware
- Denial of Service
- Phishing
- Botnet
- SQL injection

Malware

- Malicious software such as viruses, ransomware, spyware, computer worm created to harm or exploit a device or network
  - Virus. Computer code that replicates itself from device to device. Alters the way a computer operates. Needs human action to spread
  - Ransomware. Encrypts a victim's files until a ransom is paid to the attacker
  - Spyware. Aims to collect information about a victim (individual/company) and forward it to a third party without consent
  - Computer worm. Similar to virus but they spread on their own. Once in a system, a worm can, for example attach itself to an email and be delivered to all one's contacts.
- Can be used by cybercriminals to extract data they can leverage for financial gain
- Can be used to trick people into revealing personal data – identity theft
- Can be used to steal credit card or financial data
- Can be used for denial-of-service (DoS) attacks
  - DoS attack is when a computer/network is shut down or made unavailable to intended users

Preventing malware threats

- Hire cyber security experts
- Ensure cyber security updates and patches are up to date
- Use reputable antivirus and anti malware solutions
- Protect devices; keep o/s up to date, don’t click on link in popup
- Train employees on cyber security awareness so they avoid suspicious websites, emails with download links, etc.
- Limit user access and application privileges; restrict download permission to administrators
- Perform regular checks; run a scan using security software, check bank account regularly

Denial of Service

- DoS attack is when a computer/network is shut down or made unavailable to intended/legitimate users
- Cyber attackers flood computer or network with traffic so it is unable to respond or send it information that triggers a crash
- Individual networks can be affected by DoS attacks without being directly targeted
  - E.x. if a network's ISP or cloud service provider is a victim of a DoS attack, the network will experience a loss of service
- Symptoms include unusually slow network performance (opening files or accessing websites), unavailability of your website
- Detect DoS through network traffic monitoring/analysis – network administrator
- DDoS – Distributed denial of service. Same as DoS but attack is from a network of computers

Preventing DoS attacks

- Employ cyber security experts
- Sign up for DoS protection that can detect abnormal flow of traffic in your network. DoS traffic is filtered out while genuine traffic is allowed to pass through the network
- Create a disaster recovery plan to ensure recovery in a case of attack
- Install antivirus software and keep up to date
- Install firewall and configure to restrict incoming and outgoing traffic
- If experiencing DoS attack, contact network administrator; network admin can confirm if there is a DoS and identify the source and reroute traffic

Phishing

- Phishing is when a cybercriminal attempts to steal private or sensitive information from a user or a business
- Attackers use social engineering. Art of manipulating, influencing or deceiving you to gain access to your computer
- Commonly happens through fraudulent emails, text messages or social media
  - Ask you to verify your account, confirm billing address, send you a bill and ask you to verify/cancel by clicking link
- Attackers can hijack username/password
- Steal money/open credit card in one's name
- Make purchases
- Phishing emails
  - Request for confidential information
  - Use scare tactics, emotional language, portray a sense of urgency
  - Have misspelled URLs, spelling mistakes

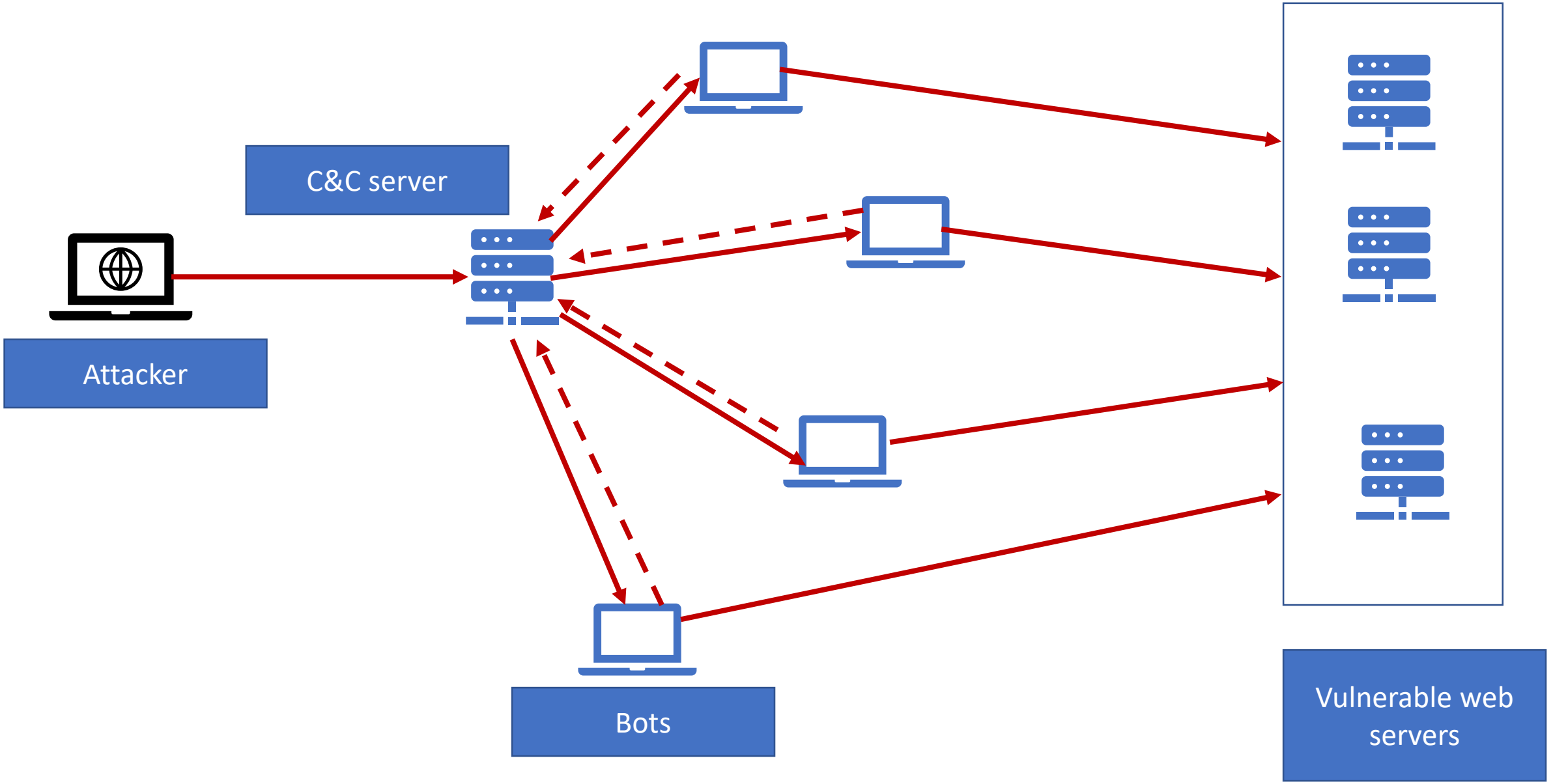
Preventing phishing attack

- Be suspicious of emails asking for personal information. Don’t provide personal information by email
- If suspicious of an email from say a bank, don’t click the link but go directly to the bank’s website or app and login from there
  - Contact the bank directly to ensure the email is legitimate
- Use varied and complex password for all your accounts or use a password management service/2 factor authentication
- Check personal accounts frequently
- A company should
  - Provide a way to report phishing emails
  - Run random phishing simulations
  - Create cyber security awareness training for employees
  - Use reliable email/spam filters
  - Require 2 factor authentication
  - Use email encryption for sensitive emails, emails with personal information

Botnet

- (Robot network), a network of computers infected by malware that are controlled by an attacker
- The attacker can use each computer on the network (bot) to simultaneously carry out criminal action like attack a company's network for financial gain
- Botnet remains under control of remote attacker, infected computers can receive updates and adapt to new instructions
- Attacker can use command and control (C&C) software
- Common actions of botnets:
  - Bulk spam emails
  - Distributed denial of service (DDoS) – most common
  - Financial breach
  - Malware

Botnet



Preventing botnet attacks

- Employ a cyber security expert
- Keep software up to date
- 24-hour monitoring of the network using analytics tools
- Monitor failed login attempts
- Use botnet detection solutions/tools

SQL injection

- Allows attacker to interfere with queries that an application makes to its database
- Attacker is able to view data that they are not normally able to retrieve – user data or data that the application can access
- Attacker can modify/delete data causing data integrity issues

SQL injection

https://somewebsite.com/products?category=Halloween

- String query = "SELECT * FROM products WHERE category = ' "+ input + " ' ";
- Application makes SQL query to database to retrieve products in Halloween category
- SELECT * FROM products WHERE category = 'Halloween' AND released = 1
- This SQL query asks the database to return:
  - all details (*)
  - from the products table
  - where the category is Halloween
  - and released is 1 – product has been released for sale, 0 – not yet released
- Hacker can construct SQL injection in the form

https://somewebsite.com/products?category=Halloween’--

- Results in query

  SELECT * FROM products WHERE category = ‘Halloween'--' AND released = 1

  -- is used for comments in SQL so rest of line from – is interpreted as comment

Database will process

  SELECT * FROM products WHERE category = ‘Halloween’

and return ALL products released or not

Preventing SQL injection vulnerabilities

- Use prepared statements - parameterized queries
- Prepared statements always treat client-supplied data as content of a parameter and never as a part of an SQL statement.
  - String query = "SELECT * FROM products WHERE category = ' "+ input + " ' ";
- Do instead
  - PreparedStatement statement = connection.prepareStatement("SELECT * FROM products WHERE category = ?");
  - statement.setString(1, input);
  - ResultSet resultSet = statement.executeQuery();

Hacking

- Intentional, unauthorized access to computer systems
- Relies on security vulnerabilities to gain unauthorized access to devices or networks
- Hackers use malware (or other types of security threats) to break into an organization's network or a personal computer
  - Malicious hackers (Black hat hackers). Usually engage in criminal activity, such as breaking into protected digital systems without permission. Aim to steal and sell data for personal financial gain or work to modify, delete, or leak valuable data to harm an organization or individual
  - Ethical hackers (White hat hackers). Use their hacking skills to identify vulnerabilities in a network and improve security
  - Hactivists. Use of hacking to promote a political cause

- Is hacking that does no direct damage a bad thing?
- Is hiring former hackers to enhance security a good thing?

Responsibility for security

- Developers have a responsibility to develop with security in mind
  - OWASP Top 10
- Companies have a responsibility to hire security personnel who can use tools to monitor their systems to prevent security attacks
- Individuals have a responsibility to secure their home networks using firewalls, anti-virus and anti-spyware. Home users also have a responsibility to be cautious when clicking on links in their emails

Laws

- 1986 Congress passed the Computer Fraud and Abuse Act (CFAA)
- US cybersecurity bill designed to address legal and illegal access to federal and financial IT systems
- The law prohibits accessing a computer without authorization
- Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet

Laws

- *“Willful interception of private communications is a criminal offence under Section 184 of the Criminal Code of Canada, RSC 1985, c C-46 (the "**Code**"), with a maximum sentence of five years' imprisonment”*
- *“Section 342.1 of the Code prohibits fraudulently obtaining any computer service or intercepting any function of a computer system. Use of a computer system with intent to commit such an offence and use or possession of a computer password to enable such an offence are also prohibited. The maximum sentence is 10 years' imprisonment.”*
- *“Hacking has also been prosecuted under*
  - *Section 380(1) of the Code, which prohibits defrauding the public or any person of property, money, valuable security or a service*
  - *Section 430 of the Code”*

Source: https://www.mondaq.com/canada/security/1012302/cybersecurity-laws-and-regulations-2021

Links

- https://www.cbc.ca/news/canada/edmonton/macewan-university-phishing-scam-edmonton-1.4270689
  - MacEwan University phishing attack
- https://www.nbcnews.com/tech/security/ubiquiti-networks-says-it-was-victim-47-million-cyber-scam-n406201
  - Ubiquiti Networks Says It Was Victim of $47 Million Cyber Scam
- https://www.cpomagazine.com/cyber-security/verizon-data-breach-report-2021-pandemic-has-caused-major-surge-in-phishing-ransomware-and-web-app-attacks/
  - Verizon’s 2021 data breach report

Verizon's 2021 data breach report

"Denial of service (DDoS) were the most common type of attack, but social engineering and basic web application attacks caused the majority of data breaches. Among these breaches, a whopping 85% were attributed to a "human element." 61% additionally involved the use of unauthorized credentials. Over 10% of data breaches involved ransomware, double the number seen in 2019."

"In addition to the spike in ransomware attempts, the count of data breaches that involved phishing rose to 36% (from 25% the previous year). But in all the incidents that involved hacking, attacks on web applications were overwhelmingly frequent (80%)."

Source: https://www.cpomagazine.com/cyber-security/verizon-data-breach-report-2021-pandemic-has-caused-major-surge-in-phishing-ransomware-and-web-app-attacks/

Summary

- Online security are the tactics/ways for protecting activities and transactions carried out online
- Online security threats include malware, Denial of Service, phishing, botnet, SQL injection
- Hacking is the use of malware to break into an organization’s network or a personal computer
- Types of hackers include malicious hackers, ethical hackers, and hacktivists
- Everyone is responsible for online security; developers, companies and individuals
- Security laws exist to protect people/companies and to prosecute cyber criminals/attackers

Reference

- *A Gift of Fire. Social, Legal and Ethical Issues for Computing Technology*. Fifth Edition. Sara Baase and Timothy M. Henry. Pearson