MOBILE DEVICES – PART 2

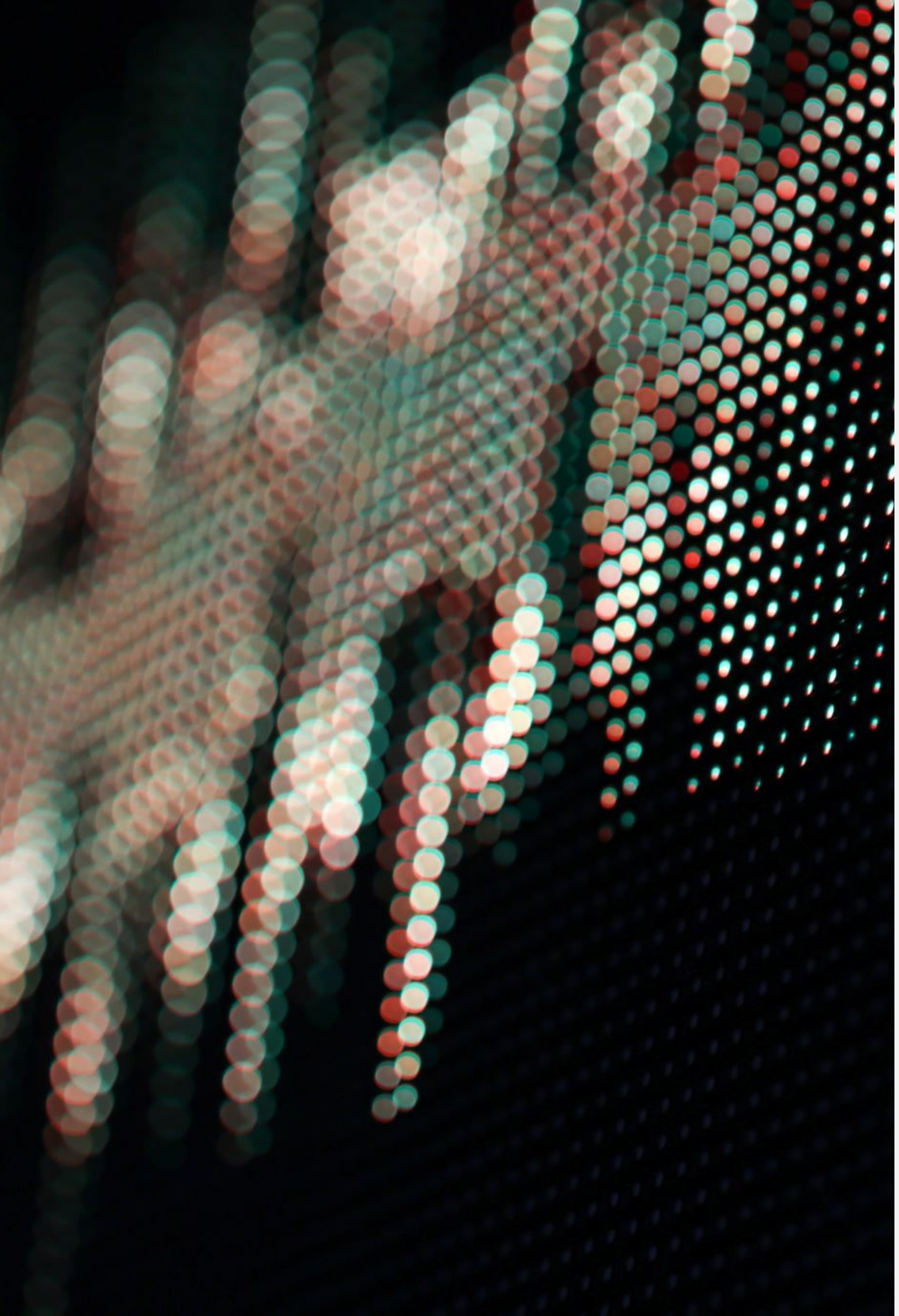
By: Dr. Fayzeh Abdulkareem Jaber

SOFTWARE FOR HOME, PERSONAL, AND EDUCATION

- Software is a collection of computer programs and associated data that provides instructions for a computer to perform a specific task. There are many different types of software, including:

SOFTWARE FOR HOME, PERSONAL, AND EDUCATION

- Application software: Helps users perform specific tasks, such as word processing, web browsing, and playing games.
- System software: Manages and controls the computer's hardware and resources.
- Programming software: Used to develop new software applications.



APPLICATION SOFTWARE FOR COMMUNICATION

Application software for communication allows users to communicate with each other electronically. Some examples include:

- Email: Allows users to send and receive messages over the internet.
- Instant messaging: Allows users to have real-time conversations with each other over the internet.
- Voice over IP (VoIP): Allows users to make and receive phone calls over the internet.
- Video conferencing: Allows users to have two-way video and audio conversations with each other over the internet.

LEARNING AND SUPPORT TOOLS FOR APPLICATION SOFTWARE

There are many different learning and support tools available for application software. Some examples include:

- User guides: Provide step-by-step instructions on how to use a software application.
- Online tutorials: Provide interactive lessons on how to use a software application.
- Online forums and communities: Allow users to ask questions and get help from other users.
- Technical support: Provided by the software developer or a third-party company.

COMPUTER SECURITY RISKS

Computer security risks are threats that can damage or destroy computer systems, networks, or data. Some common computer security risks include:

- Malware: Malicious software, such as viruses, worms, and Trojan horses.
- Phishing: Emails or websites that try to trick users into revealing personal information.
- Hacking: Unauthorized access to computer systems or networks.
- Denial-of-service attacks: Attacks that attempt to make computer systems or networks unavailable to users.

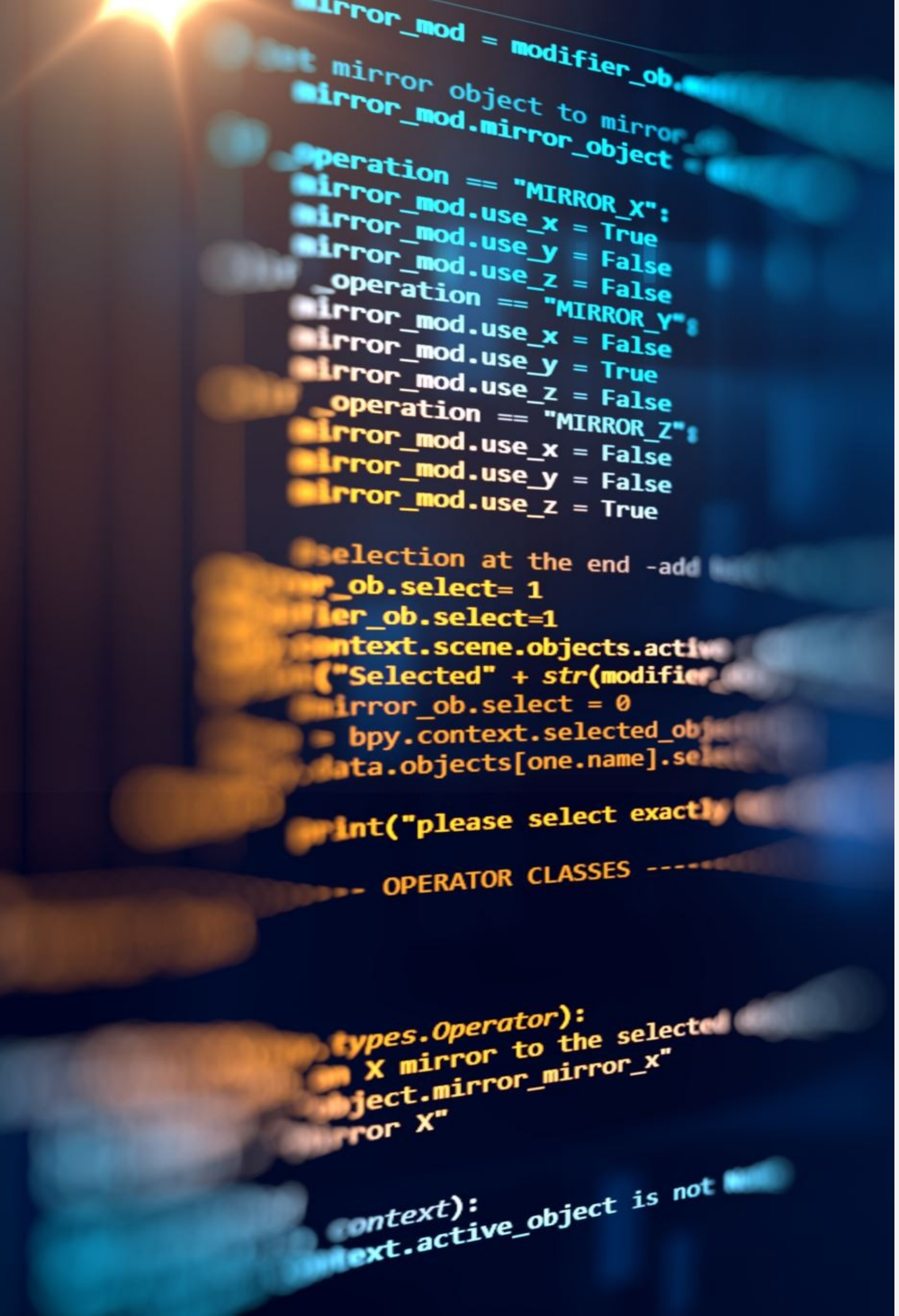
INTERNET AND NETWORK ATTACKS

internet and network attacks are attacking that target computer systems or networks that are connected to the internet. Some common internet and network attacks include:

- Man-in-the-middle attacks: Attacks that intercept communications between two parties and impersonate one of the parties.
- DNS poisoning attacks: Attacks that redirect users to malicious websites.
- Distributed denial-of-service (DDoS) attacks: Attacks that overwhelm computer systems or networks with traffic, making them unavailable to users.

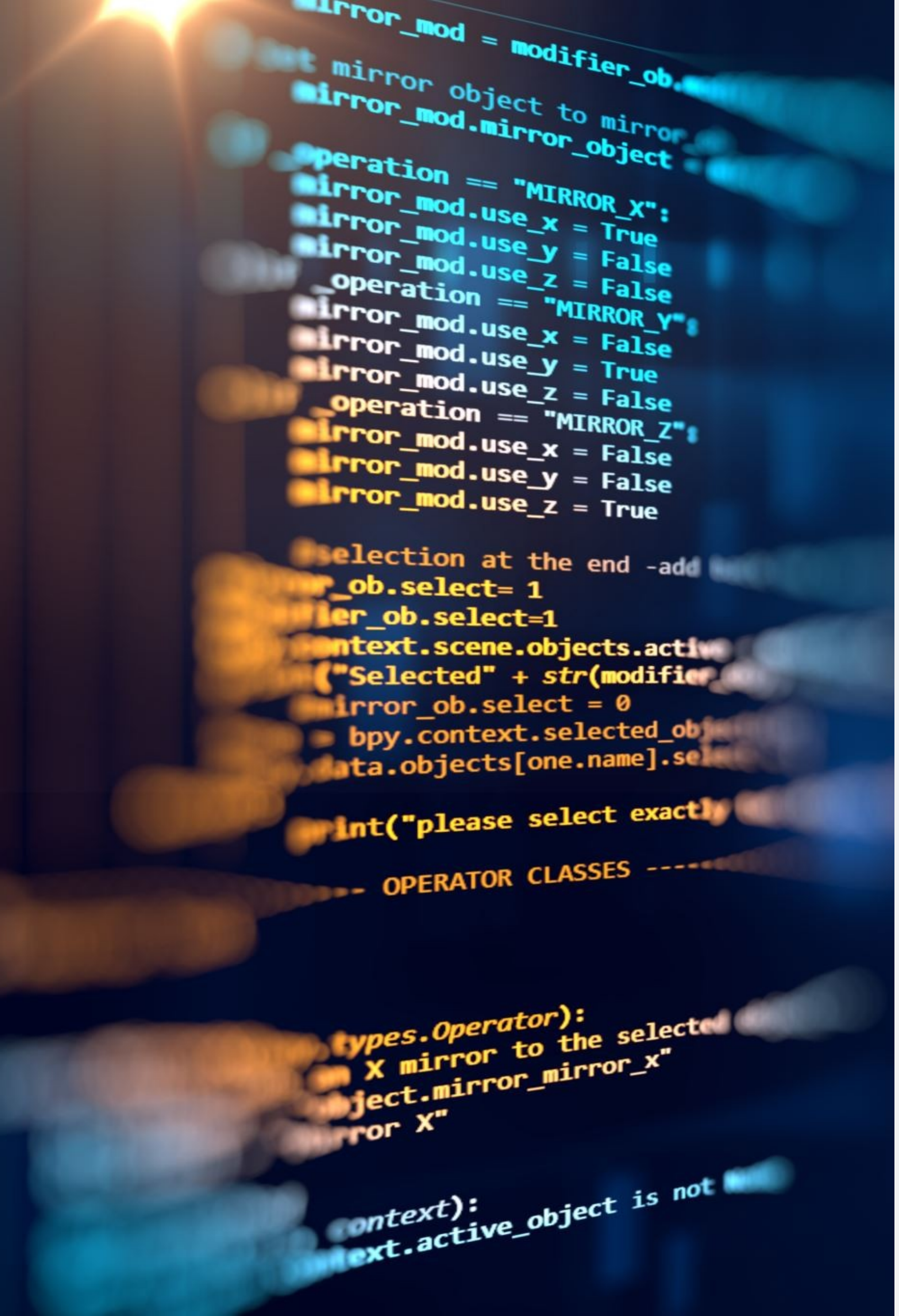
UNAUTHORIZED ACCESS AND USE

- Unauthorized access and use is the unauthorized use of computer systems, networks, or data. This can include using a computer system or network without permission, or accessing data that you are not authorized to access.



HARDWARE THEFT AND VANDALISM

- Hardware theft and vandalism is the unauthorized taking or destruction of computer hardware. This can include stealing laptops, desktops, servers, or other computer equipment.



SOFTWARE THEFT

- Software theft is the unauthorized copying or use of software. This can include copying software without a license, or using software that has been cracked or pirated.

CONCLUSION

Computer security is important for everyone, regardless of whether you use a computer for home, personal, or educational purposes. There are many things you can do to protect your computer systems, networks, and data from security risks, such as:

- Installing and maintaining security software
- Using strong passwords and multi-factor authentication
- Being careful about what emails you open and what websites you visit
- Keeping your software up to date

CASE STUDY

SCENARIO

- A university student named Alice is working on a research paper for her computer science class. She needs to find some information on the latest cyber security threats. She decides to do a Google search and clicks on the first link that comes up.
- The website she visits looks like a legitimate news website, but it is actually a phishing website. Phishing websites are designed to trick users into revealing their personal information, such as their passwords and credit card numbers.
- Alice enters her university login credentials into the phishing website without thinking. The next day, she tries to log into her university account, but she can't. She realizes that her account has been compromised.

QUESTIONS

1. What mistake did Alice make?
2. How could Alice have avoided this mistake?
3. What are the consequences of Alice's mistake?

ANSWERS

1. Alice clicked on a link to a phishing website.
2. Alice could have avoided this mistake by being more careful about what links she clicks on. She should only click on links from trusted sources. She can also hover over links to see the real URL before clicking.
3. The consequences of Alice's mistake are that her university account has been compromised and her personal information could be stolen.

SCENARIO 2

- A small business owner named Bob has a website where he sells his products. He has not taken any steps to protect his website from cyber security threats.
- One day, Bob's website is hacked by a group of cyber criminals. The cyber criminals install malware on the website that steals the personal information of Bob's customers, including their credit card numbers and social security numbers.
- Bob's customers start to receive fraudulent charges on their credit cards. They also start to receive notifications from the IRS about suspicious activity on their tax accounts.

QUESTIONS

1. What mistakes did Bob make?
2. How could Bob have avoided these mistakes?
3. What are the consequences of Bob's mistakes?

ANSWERS

1. Bob did not take any steps to protect his website from cyber security threats.
2. Bob could have avoided these mistakes by installing security software on his website and keeping it up to date. He could have also used strong passwords and enabled multi-factor authentication on his website.
3. The consequences of Bob's mistakes are that his customers' personal information has been stolen and they could be victims of identity theft. Bob could also be held liable for the damages caused to his customers.

END