Instructors Guide

On the following pages is a sample module from our Instructor Guide. It provides the instructor with a copy of the material and a Lesson Plans box.

The key benefit for the trainer is the Lesson Plan box. It provides a standardized set of tools to assist the instructor for each lesson. The Lesson Plan box gives an estimated time to complete the lesson, any materials that are needed for the lesson, recommended activities, and additional points to assist in delivering the lessons such as Stories to Share and Delivery Tips.

U.S. computer networks and databases are under daily cyber-attack by nation states, international crime organizations, subnational groups, and individual hackers.

John O. Brennan

Module Two: Cyber Security Fundamentals

Bloom's Taxonomy has been a basis for educators since its inception. Teachers of children and adults should be familiar with the theory's history and how it has changed over the years. In this manual, the focus is on the psychomotor domain.

What is Cyberspace?

Cyberspace is the environment where computer transactions take place. This specifically refers to computer-to-computer activity. Although there is no "physical" space that makes up cyberspace, with the stroke of a few keys on a keyboard, one can connect with others around the world.

Examples of items included in cyberspace are:

- Networks
- Devices
- Software
- Processes
- Information storage
- Applications

Estimated Time	**7 minutes**
Topic Objective	Review the definition of cyberspace.

© Global Courseware

Topic Summary	**What is Cyberspace?** Discuss what cyberspace is.
Materials Required	**Flipchart/board, marker**
Planning Checklist	None
Recommended Activity	As a group, discuss the examples of items included in cyberspace. Consider how they work within cyberspace. Write answers on the board/flipchart.
Stories to Share	Share any personal, relevant stories.
Delivery Tips	Encourage everyone to participate.
Review Questions	How is software considered a part of cyberspace?

What is Cyber Security?

As previously mentioned, cyber security is the implementation of methods to prevent attacks on a company's information systems. This is done to avoid disruption of the company's productivity. Not only does cyber security include controlling physical access to the system's hardware, it protects from danger that may come via network access or the injection of code.

Estimated Time	**7 minutes**
Topic Objective	Review the definition of cyber security.
Topic Summary	**What is Cyber security?** Discuss how cyber security can protect a system's hardware and danger that can come in via network access and code injection.
Materials Required	**Flipchart/board, marker**
Planning Checklist	None
Recommended Activity	As a group, using the flipchart/board, come up with and write down participants' personal definitions of cyber security.
Stories to Share	Share any personal, relevant stories.

Delivery Tips	Encourage everyone to participate.
Review Questions	What can cyber security protect?

Why is Cyber Security Important?

Cyber security is crucial to a business for a myriad of reasons. The two this section will focus on are data security breaches and sabotage. Each can have dire effects on a company and/or its clients.

Data security breaches can compromise secure information such as:

- Names and social security numbers
- Credit card and bank details
- Trade secrets
- Intellectual property

Computer sabotage serves to disable a company's computers or network to impede the company's ability to conduct business.

Estimated Time	**7 minutes**
Topic Objective	Review the data security breaches and computer sabotage.
Topic Summary	**Why is Cyber security Important?** Recognize the benefits of utilizing cyber security.
Materials Required	**Worksheet 1: Data Security Breaches**
Planning Checklist	None
Recommended Activity	Complete the worksheet individually. Share your answers with the rest of the group.
Stories to Share	Share any personal, relevant stories.
Delivery Tips	Encourage everyone to participate.
Review Questions	None

What is a Hacker?

In simple terms, a hacker is an individual, or group of individuals, who use their knowledge of technology to break into computer systems and networks, using a variety of tools to gain access to, and utilize other people's data for devious reasons.

There are 3 main types of hackers. They are:

- Grey hats: These hackers do so "for the fun of it".
- Black hats: These hackers have malevolent reasons for doing so, such as stealing and/or selling data for monetary gain.
- White hats: These hackers are employed by companies to hack into systems to find where the company is vulnerable, with the intention of ensuring the safety of the data from hackers with ill intentions.

Estimated Time	**7 minutes**
Topic Objective	Review the definition of a hacker.
Topic Summary	**What is a Hacker?** Recognize what a hacker is and why they are dangerous.
Materials Required	**Worksheet 2: Hacker**
Planning Checklist	None
Recommended Activity	Complete the worksheet individually. Share your answers with the rest of the group.
Stories to Share	Share any personal, relevant stories.
Delivery Tips	Encourage everyone to participate.
Review Questions	What is the main difference between a black hat and a white hat?

Practical Illustration

Patrick and Willow are in the process of opening a small answering service business. They are discussing the various needs of the company, including the type of security they are going to use for their computer systems. Patrick tells Willow that he doesn’t believe it’s necessary to implement any type of computer security because their business is small. Willow states even though their business will start out small, they are still vulnerable and there are many hackers out there that can break into their system and disrupt business.

© Global Courseware

Module Two: Review Questions

1.) Cyberspace refers to which of the following?

a) Computer-to-computer activity
b) Individual-to-individual activity
c) Supervisor-to-employee activity
d) Computer-to-physical location activity

Cyberspace is not a physical location. It is an environment where computer transactions take place.

2.) What is an item that is included in cyberspace?

a) Network
b) Software
c) Application
d) All of the above

In addition to the above, devices, processes, and information storage are a part of cyberspace.

3.) Why is cyber security implemented?

a) To speed up the network of a company's computers
b) To avoid the disruption of a company's business
c) To increase the number of clients a company has
d) To lessen the number of employees a company employs

Cyber security helps companies avoid disruption inflicted by hackers, thus not slowing down the company's productivity.

4.) Cyber security helps control physical access to and prevents danger that may come in from:

a) Hardware
b) Network access
c) Code injection
d) All of the above

This helps prevent damage to the company's entire information systems.

5.) What type of information is NOT secure information that is likely to be compromised in a data security breach?

a) Intellectual property
b) Credit card information
c) The name of a company’s CEO
d) Social security numbers

The name of a company’s CEO is public information. Information that is not considered public, such as names and social security numbers and bank details could fall victim to a data security breach.

6.) What is the main purpose of computer sabotage?

a) To disable a company’s computers or networks to prevent it from conducting business.
b) To disable a company’s computers or networks to prevent it from being able to obtain a business license.
c) To disable a company’s computers or networks to prevent it from being able to hire employees.
d) To disable a company’s computers or networks to prevent it from being able to give its employees raises.

Data security breaches and sabotage can both have dire effects on a company and/or its clients.

7.) Why do “grey hat” hackers typically hack into computers?

a) To steal data for monetary gain
b) For the fun of it
c) To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them
d) To sell data for monetary gain

There are three types of hacker:

Grey hats: These hackers do so “for the fun of it”.

Black hats: These hackers have malevolent reasons for doing so, such as stealing and/or selling data for monetary gain.

White hats: These hackers are employed by companies to hack into systems to find where the company is vulnerable, with the intention of ensuring the safety of the data from hackers with ill intentions.

8.) Why do “white hat” hackers typically hack into computers?

a) To steal data for monetary gain
b) For the fun of it
c) To find vulnerabilities in a computer system so the company can fix them before hackers with bad intentions can exploit them
d) To sell data for monetary gain

There are three types of hackers:

Grey hats: These hackers do so “for the fun of it”.

Black hats: These hackers have malevolent reasons for doing so, such as stealing and/or selling data for monetary gain.

White hats: These hackers are employed by companies to hack into systems to find where the company is vulnerable, with the intention of ensuring the safety of the data from hackers with ill intentions.

9.) The method(s) of cyber security that a company uses should be tailored to fit the needs of the _________.

a) Hacker
b) Employees
c) Organization
d) Manager

The method(s) of cyber security that a company uses should be tailored to fit the needs of the organization.

10.)___________ is the environment where computer transactions take place.

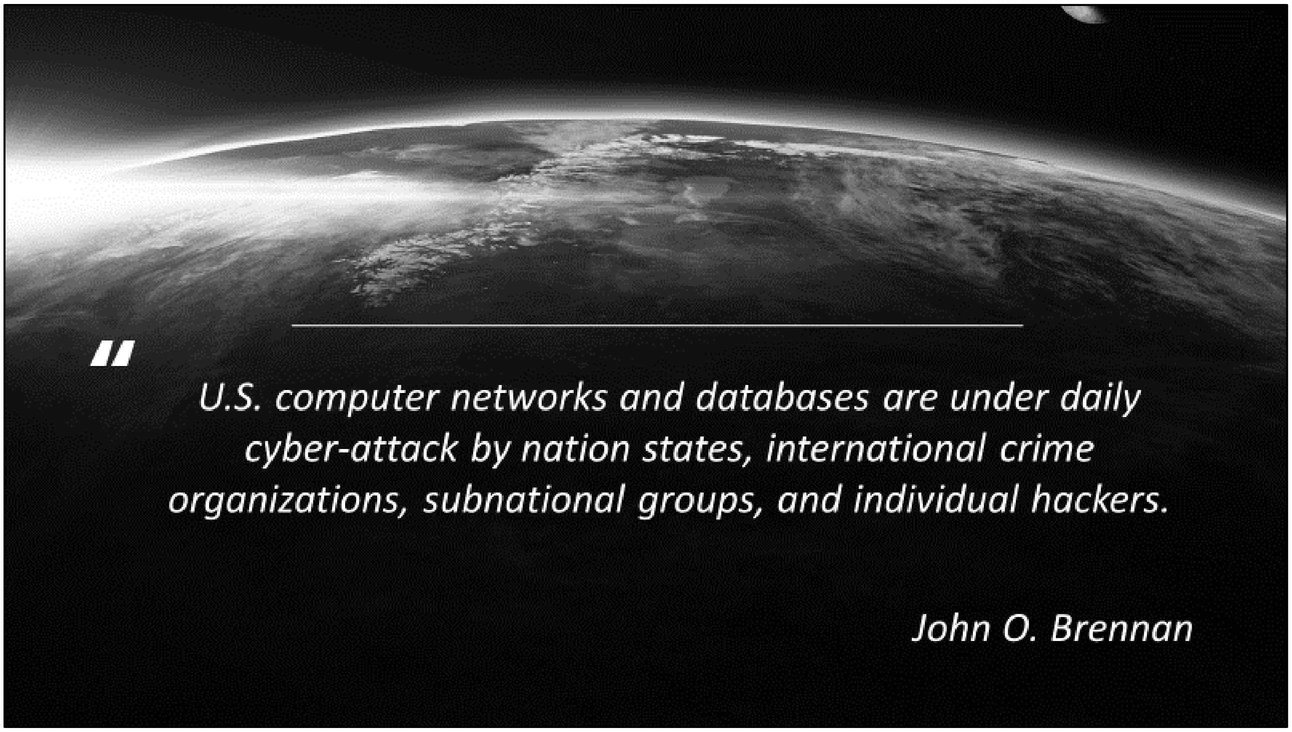
a) An office
b) Cyberspace
c) A mall
d) None of the above

Cyberspace is the environment where computer transactions take place.

PowerPoint Slides

Below you will find the PowerPoint sample. The slides are based on and created from the Instructor Guide.

PowerPoint slides are a great tool to use during the facilitation of the material; they help to focus on the important points of information presented during the training.



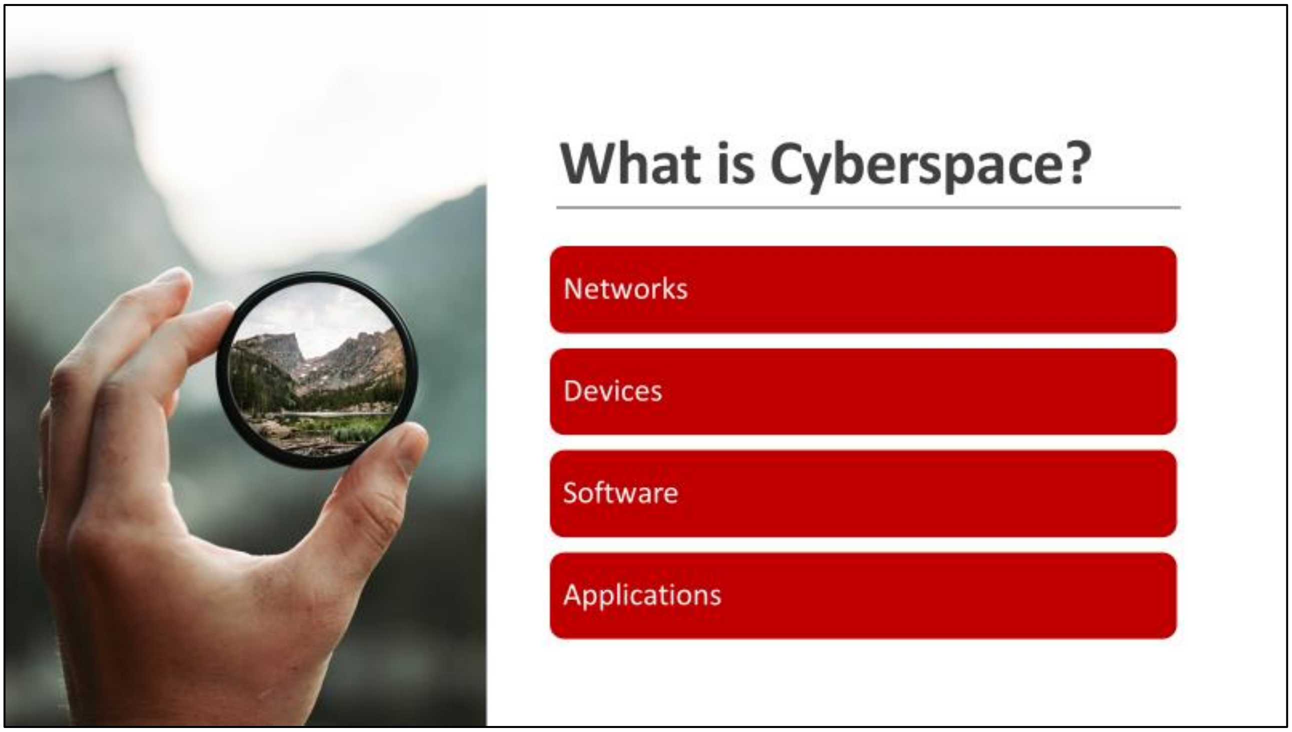
> “ U.S. computer networks and databases are under daily cyber-attack by nation states, international crime organizations, subnational groups, and individual hackers.
>
> *John O. Brennan*

MODULE TWO

Cyber Security Fundamentals

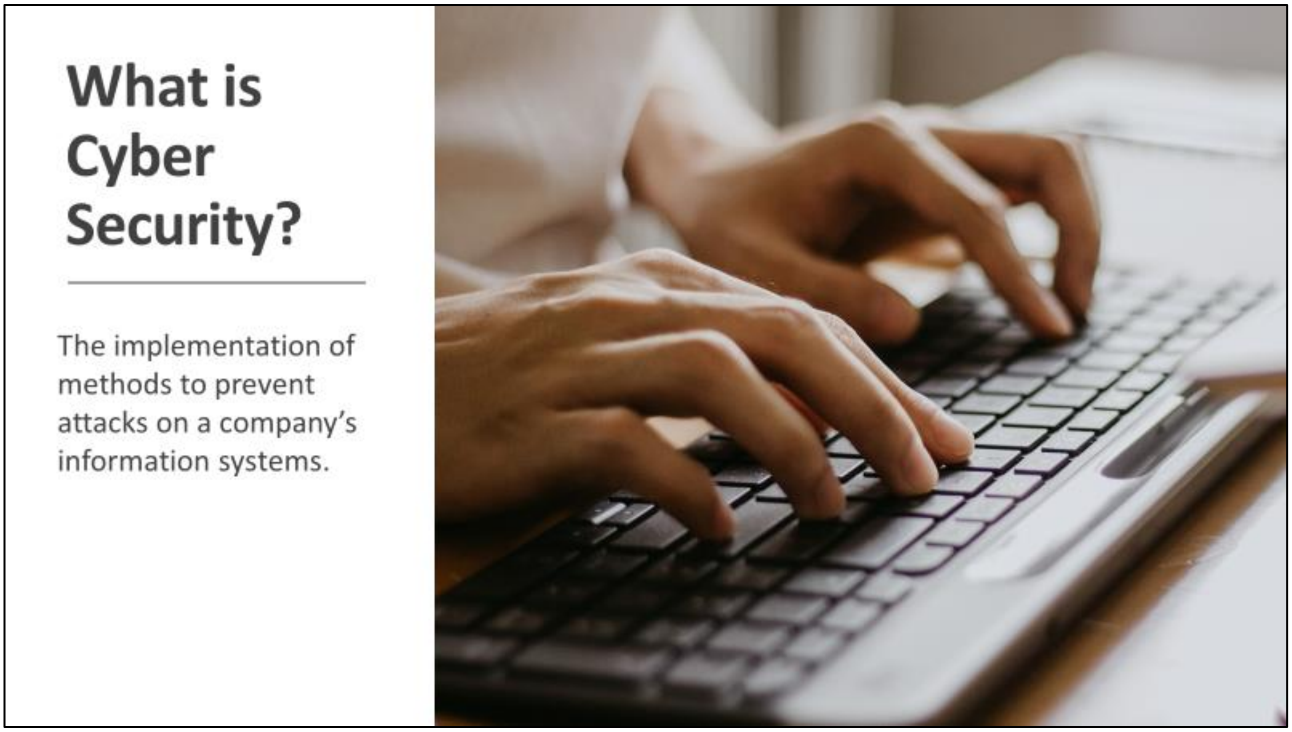
Before developing and implementing security measures to prevent cyberattacks, you must understand basic concepts associated with cyber security and what cyberattacks are.

© Global Courseware



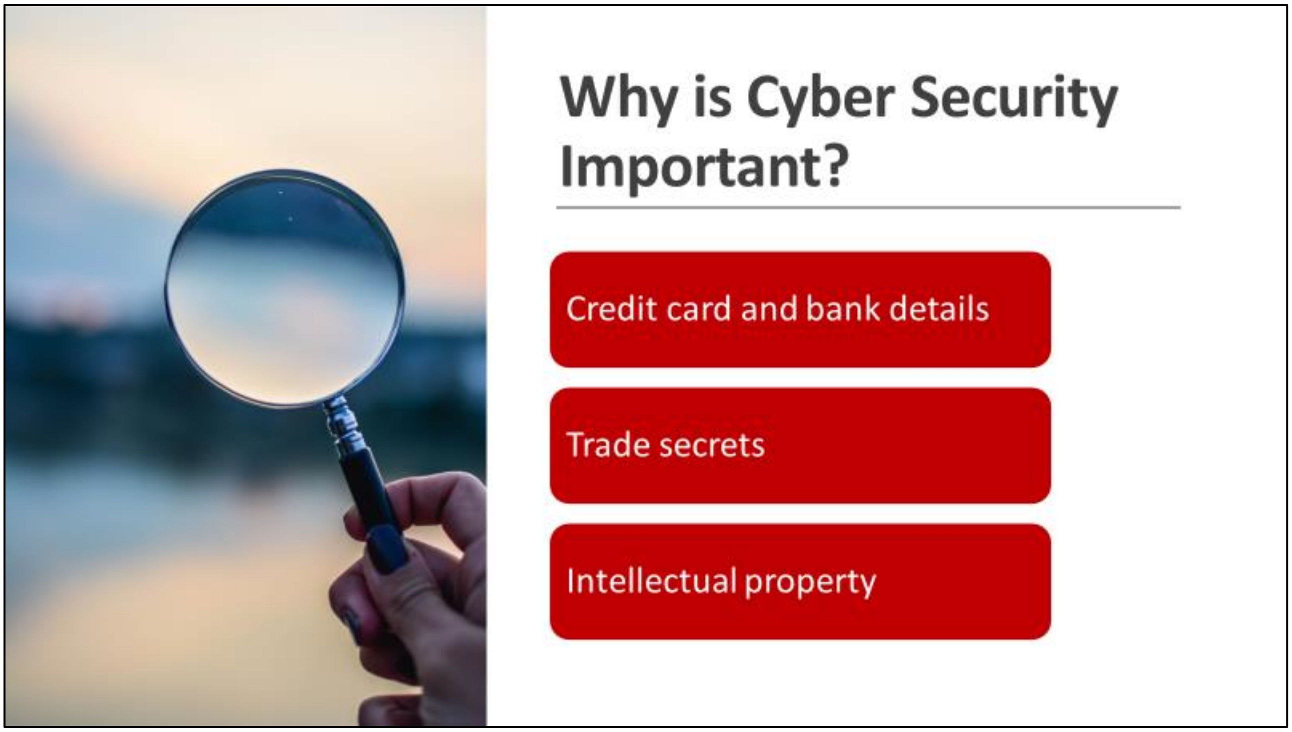
What is Cyberspace?

- Networks
- Devices
- Software
- Applications



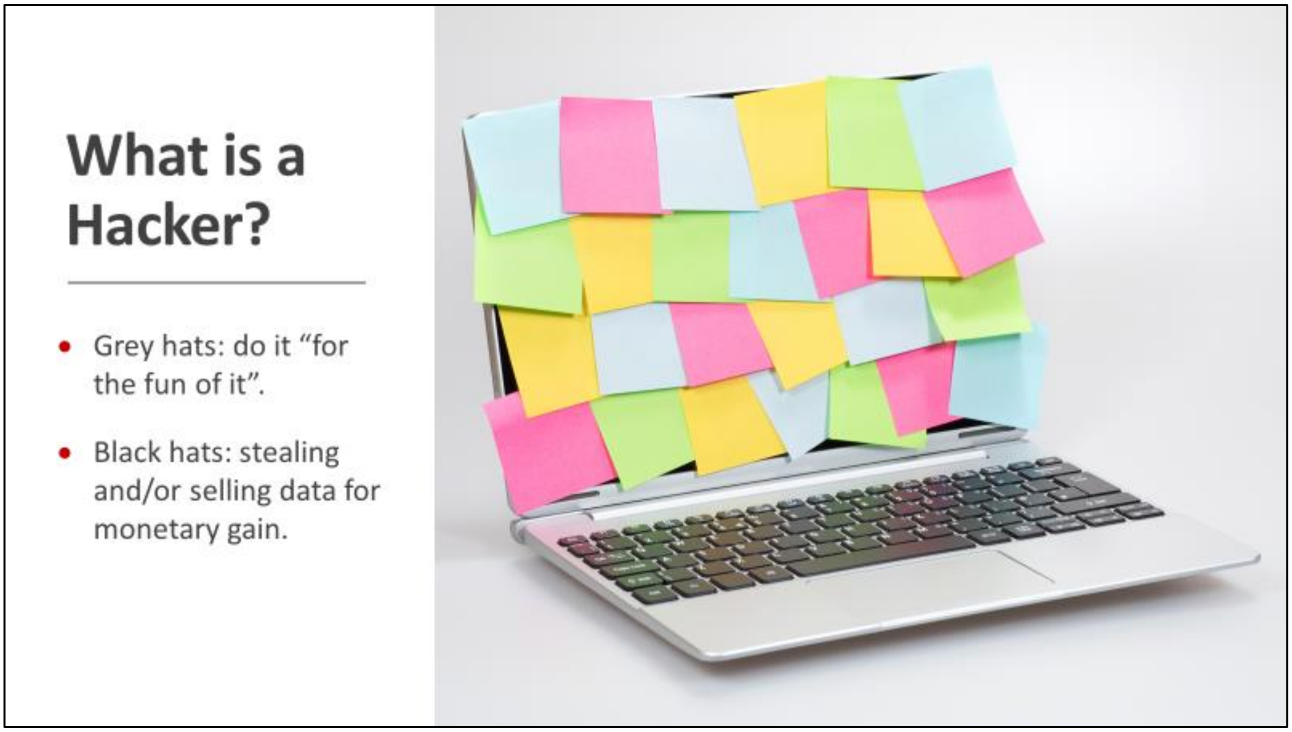
What is Cyber Security?

The implementation of methods to prevent attacks on a company's information systems.



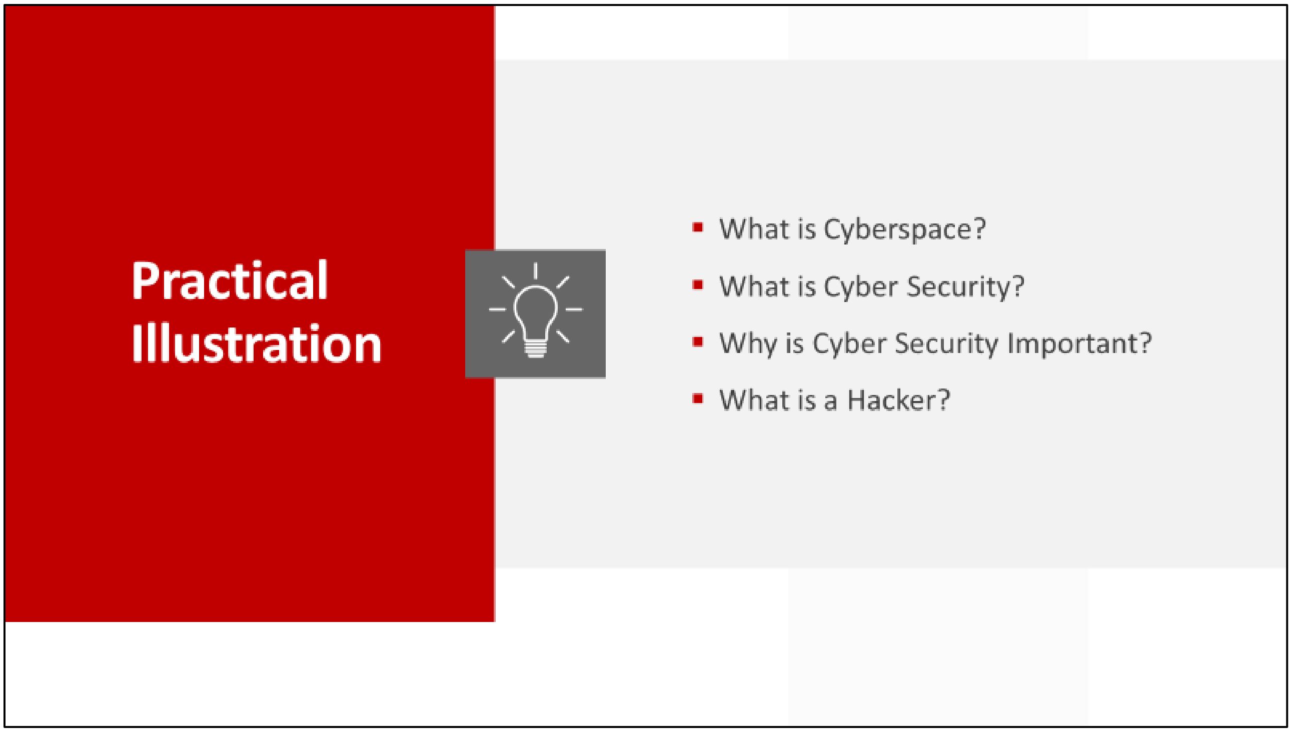
Why is Cyber Security Important?

- Credit card and bank details
- Trade secrets
- Intellectual property



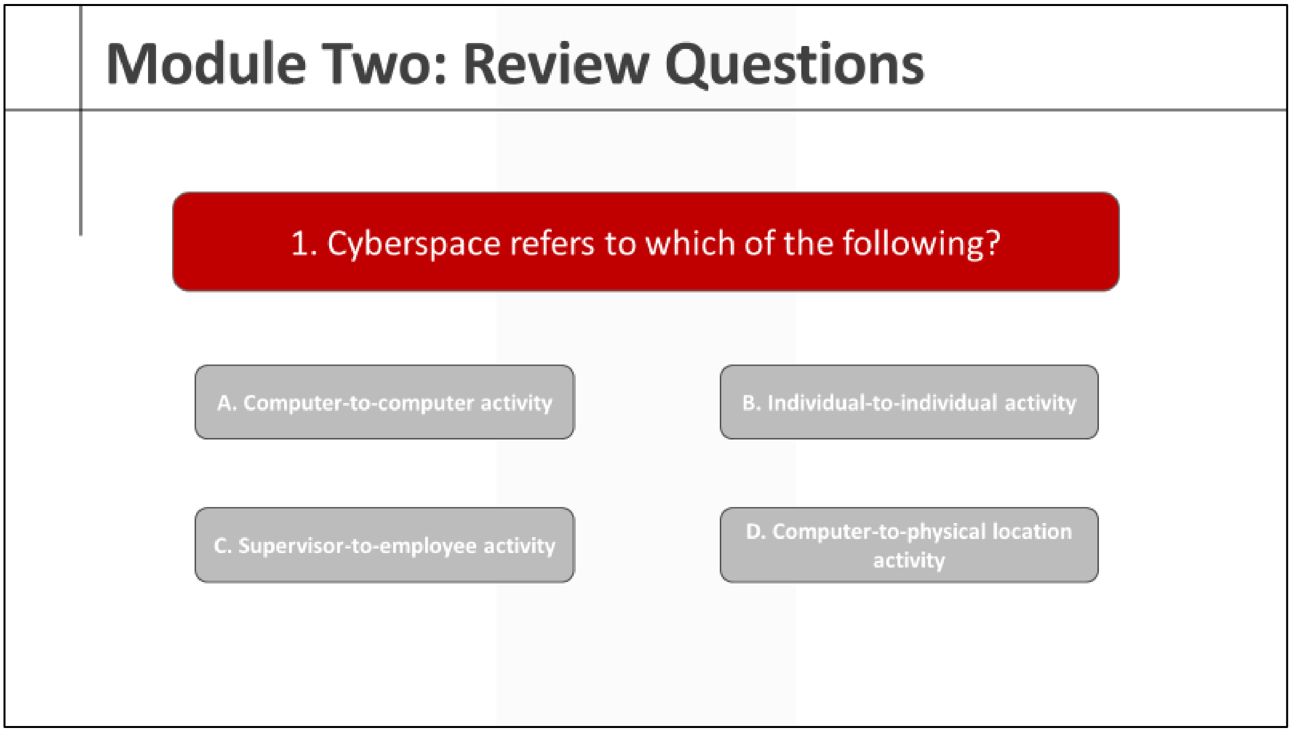
What is a Hacker?

- Grey hats: do it "for the fun of it".
- Black hats: stealing and/or selling data for monetary gain.



Practical Illustration

- What is Cyberspace?
- What is Cyber Security?
- Why is Cyber Security Important?
- What is a Hacker?



Module Two: Review Questions

1. Cyberspace refers to which of the following?

A. Computer-to-computer activity

B. Individual-to-individual activity

C. Supervisor-to-employee activity

D. Computer-to-physical location activity

© Global Courseware

Quick Reference Sheets

Below is an example of our Quick Reference Sheets. They are used to provide the participants with a quick way to reference the material after the course has been completed.

They can be customized by the trainer to provide the material deemed the most important.

They are a way the participants can look back and reference the material at a later date.

They are also very useful as a take-away from the workshop when branded. When a participant leaves with a Quick Reference Sheet it provides a great way to promote future business.

Cybersecurity
Quick Reference Sheet

Why is Cybersecurity Important?

Cybersecurity is crucial to a business for a myriad of reasons. The two this section will focus on are data security breaches and sabotage. Both can have dire effects on a company and/or its clients.

Data security breaches can compromise secure information such as:

Names and social security numbers

Credit card and bank details

Trade secrets

Intellectual property

Computer sabotage serves to disable a company's computers or network to impede the company's ability to conduct business.

Phishing

Cybercriminals who use phishing scams aim to obtain personal information by appearing to be a legitimate source. Many times, they masquerade as a major company, such as a bank, appealing to your desire to keep your information safe.

For example, they may send an email that says, "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

Clicking the link or responding to the email can take you to a website that looks authentic, but is in fact a spoof site that serves to steal your information and use it for malicious purposes, such as commit crimes using your name, or using your bank information for personal gain.

© Global Courseware

Cryptography

Cryptography is basically defined as a secret method of writing. This is done so that only authorized parties are able to interpret the message. It is used in various industries, such as banking and health to protect the privacy and security of companies and customers'/patients' information. Examples of encryption methods include:

- International Data Encryption Method (IDEA)
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)

Handouts

Each course is provided with a wide range of worksheets. Worksheets help check your participants' understanding. If a lesson calls for a worksheet, it will be listed in the Lesson Plan box under Materials Required. All worksheets are customizable and can be found in the Appendix of the Instructor Guide and the Training Manual.

As a trainer, icebreakers give your participants the opportunity to get to know each other better or simply begin the training session on a positive note. Icebreakers promote collaboration, increase engagement, and make your training more light-hearted and fun. Below is an example from the Icebreakers folder.

Sample Worksheet 1

Data Security Breaches

Create a list of information that is used in security data breaches.

The first one has been provided for you.

1. Customer's social security number
2.
3.
4.
5.
6.
7.
8.
9.
10.

Sample Worksheet 2

Hacker

Without re-reading the lesson, define the different types of hackers.

Grey hats

Black hats

White hats

© Global Courseware

Icebreaker: Related Topic

Include a short activity here that is related to the topic of the workshop. You can use the one below if you like.

1. Have the participants at each table answer the following questions:

    a. Why are they here?

    b. What is their level of experience with Cyber Security?

    c. What they hope to get from this class?

    d. What was their most memorable vacation or trip?

2. Have someone be designated a scribe and have them jot down the answers to question C above.

3. On a separate piece of paper, have the scribe write down the most interesting or exotic vacation or trip from only one table member.

4. Have the scribe hand the note with the answers to question C to you.

5. Have the scribe stand and introduce the table to the class.

6. Then have the scribe share the most interesting vacation or trip from their group.

7. Have the class guess the person that had the most interesting or exotic trip or vacation.

8. Go around to each table until all have given you their answers to question C and shared their most interesting trip or vacation.

9. Debrief by sharing all the answers to question C with the class.

10. Thank participants for sharing.

Certificate of Completion

Every course comes with a Certificate of Completion where the participants can be recognized for completing the course. It provides a record of their attendance and to be recognized for their participation in the workshop.

CERTIFICATE OF COMPLETION

[Name]

Has mastered the course

Cyber Security

Awarded this ________ day of _______e_____, 20___

Presenter Name and Title

____