ASU Information Security Training Refresher(2) - July 2018 -- June 2019 TRN-FY2019-AIST2-UTO

Review Test Submission: Quiz FY2019

User	Muhammed Kilig
Course	ASU Information Security Training Refresher(2) - July 2018 -- June 2019
Test	Quiz FY2019
Started	1/2/19 10:05 AM
Submitted	1/2/19 10:10 AM
Status	Completed
Attempt Score	15 out of 15 points
Time Elapsed	4 minutes
Instructions	To get credit for taking this course, you must answer 12 or more questions correctly. You may take this quiz multiple times in order to pass.
Results Displayed	All Answers, Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

Question 1

1 out of 1 points

✓ Ransomware is...

Selected Answer: ✓ B.
...a cyber attack that prevents a victim from accessing his or her own data or system until a ransom is paid.

Answers: A.
...an information security term that describes a certain type of attack vector used by hackers to gain access to a network.

✓ B.
...a cyber attack that prevents a victim from accessing his or her own data or system until a ransom is paid.

C.
...a tool used to encrypt and protect data from being stolen or held for a ransom.

Response Feedback: Correct!

blackmail you into paying a ransom to get your data or access to a particular service back.

Question 2

1 out of 1 points

If you fall victim to ransomware, which steps should you take next?

Selected Answer: ✓ D. All the above.

Answers:

A. Notify your department and the ASU information security team. Don't pay the ransom.

B. Disconnect your computer from all networks immediately, to keep the issue from spreading.

C. Work with the Information security office and your deskside support staff to resolve the situation and restore your system. This is why those backups are so important!

✓ D. All the above.

Response Feedback: Correct!

if you do fall victim to ransomware...
1) Notify your department and the ASU information security team. Don't pay the ransom

2) Disconnecting your computer from all networks immediately, to keep the issue from spreading.

3) Work with Information and your deskside support staff to resolve the situation and restore your system. This is why those backups are so important!

Question 3

1 out of 1 points

What can you do to protect your passwords, the keys to your digital assets?

(click all that apply)

Selected Answers: ✓ A. Avoid sharing personal information that a social media "friend" could use to guess the answers to your online account's security questions.

Be protective of your passwords. Never share them. Never email them. If you must write them down, don't leave the written information anywhere that is easily accessible by others.

✓ C.
Use different passwords for different accounts, just like you use different keys for different locks.

✓ D.
Create a hard-to-guess passphrase that consists of upper/lowercase letters, symbols and numbers.

Answers: ✓ A.
Avoid sharing personal information that a social media "friend" could use to guess the answers to your online account's security questions.

✓ B.
Be protective of your passwords. Never share them. Never email them. If you must write them down, don't leave the written information anywhere that is easily accessible by others.

✓ C.
Use different passwords for different accounts, just like you use different keys for different locks.

✓ D.
Create a hard-to-guess passphrase that consists of upper/lowercase letters, symbols and numbers.

Response Feedback: Correct!

All of these practices lead to good password management.

Question 4

1 out of 1 points

What is true about Two Factor Authentication at ASU?

Selected Answer: ✓ D. Both A & B are correct.

Answers: A.
Two factor authentication uses something you know (your password) and something you have (like your phone or a hardware token) to make it harder to compromise your account.

B.
It is a security measure that is required for all staff, faculty and student workers.

C.
It represents the binary but opposite (dual) principles of password complexity: Your password has to be hard to guess but simple to memorize

Response Feedback: Correct!

Two Factor authentication protects you by asking for your password and an interaction with something physical that you own. You will need to use this to access MyASU.

Question 5

1 out of 1 points

Requirements listed in ASU's Computer, Internet, and Electronic Communications Information Management Policy include...

Selected Answer: ✓ D. all of these and much more.

Answers: A. ...compliance with all applicable local, state, and federal laws and regulations, and with ASU and ABOR policies.

B. ...notifying the Information Security Office if you become aware of a security concern.

C. ...not sharing your password or letting others use your access to ASU resources.

✓ D. all of these and much more.

Response Feedback: Correct!

ASU's Computer, Internet, and Electronic Communications Information Management Policy, ACD125, defines the boundaries of acceptable use of ASU computing and communication resources. Following ACD125 helps you to get your work done safely, efficiently, a[illegible] with legal requirements and policies. Please read the policy online at http://links.asu.edu/acd125.

Question 6

1 out of 1 points

ASU's privacy policy...

Selected Answer: ✓ C. ...describes the data we collect and how we use it.

Answers: A. ...is only available by request to the General Counsel, because it's private.

...defines the boundaries of acceptable use of ASU computing and communication resources.

✓ C. ...describes the data we collect and how we use it.

D. ...is known as ACD125.

Response Feedback: Correct!

ASU's privacy policy is available in the footer of every ASU Web page. The policy describes the data we collect and how we use it to provide services consistent with ASU's charter and mission.

Question 7

1 out of 1 points

✓ Examples of PII include...

Selected Answer: ✓ D. Both A & B are correct.

Answers:

A. ...Financial Records.

B. ...Health Care Records.

C. None of the above.

✓ D. Both A & B are correct.

Response Feedback: Correct!

Sensitive data includes:

- Personally Identifying Information (known as PII) such as financial, health, and academic information...
- Cardholder Data related to payment transa
- Intellectual property, human subjects research, and even information related to national security

ASU Home My ASU Colleges & Schools Map & Locations Contact Us Muhammed Kilig

Question 8

1 out of 1 points

✓ What two major requirements apply to nearly all types of sensitive information?

(Choose all that apply)

✓ B. Encrypt everything.

✓ C. Store data in an enterprise level document storage location.

Answers: A. Store sensitive information locally to make it as secure as possible.

Encrypt everything

Response Feedback: Correct!

Two major requirements apply to nearly all types of sensitive information: Store data in an enterprise document storage location, not locally, and encrypt it.

Question 9

1 out of 1 points

What is the proper way to report a potential information security incident?

Selected Answer: ✓ D.
Contact the ASU Help Center at 1-855-278-5080 or notify the information security office at infosec@asu.edu

Answers:

A. Email help@asu.edu.

B. Dial 9-1-1.

C. Email support@asu.edu.

✓ D.
Contact the ASU Help Center at 1-855-278-5080 or notify the information security office at infosec@asu.edu

Response Feedback: Correct!

If you suspect a problem,report it to the ASU Help Center at 1-855-278-5080. The Information Security Office will help to evaluate the situation.

Question 10

Which of the following could be classified as a significant security incident?

Selected Answer: ✓ D.
All of these could potentially be considered significant security incidents.

Answers:

A.
A file that contains sensitive information is accidentally sent to a recipient who is not authorized to view the information.

B.
An instructor's account is compromised, and the instructor is unable to conduct class activities during this time.

C.
An attack brings down the main ASU website, affecting ASU's reputation.

Response Feedback: Correct!

A significant incident is an incident that may harm ASU's assets, including sensitive data, critical university business, or ASU's reputation.

Question 11

1 out of 1 points

✓ If you have an IOT or internet connected device, what should you do?

Selected Answer: ✓ D. B and C are correct.

Answers:

A. Just use it. It's a smart device, so it should be good to go.

B. Contact your local tech support, as needed, to help you encrypt and secure it.

C. Make sure the device is properly secured and that it is only monitoring and transmitting the right data.

✓ D. B and C are correct.

Response Feedback: Correct!

Question 12

1 out of 1 points

✓ What are some easy steps you can do to secure your smart (internet connected) devices?

ASU Home My ASU Colleges & Schools Map & Locations Contact Us Muhammed Kilig

Selected Answer: ✓ D. All of the above are correct.

Answers:

A. Change the password from the manufacturer's default, as default passwords can be easily searched online.

B. Keep the device patched and updated, preferably automatically.

C. Restrict access to the device and turn off remote management if you don’t need it.

✓ D. All of the above are correct.

Response Feedback: Correct!

Question 13

1 out of 1 points

✓ What should you do when you leave your desk or workspace?

Selected Answer: ✓ D. All of the above are correct.

Answers:

A. Ensure any computer systems or devices that remain are password protected or locked up.

B. Stow any sensitive documents in locked drawers.

C. Make sure laptops are physically secured by a cable lock or locked up.

✓ D. All of the above are correct.

Response Feedback: Correct!

Each time you leave your desk or workspace, you should make sure to lock up your computer, tablet, phone, and any other valuable electronic device, lock sensitive documents in an office or drawer, and use a cable lock to prevent theft.

Question 14

1 out of 1 points

✓ A privacy screen is...

Selected Answer: ✓ C. ...a plastic screen that fits over a monitor or screen and makes it so the screen can only be seen directly from the front.

ASU Home My ASU Colleges & Schools Map & Locations Contact Us Muhammed Kilig

Answers:

A. ...a fancy name for the window shades on airplanes.

B. ...an app that verifies the privacy settings on your device.

✓ C. ...a plastic screen that fits over a monitor or screen and makes it so the screen can only be seen directly from the front.

D. ...part of a background check process.

Response Feedback: Correct!

A privacy screen, or plastic device that makes it so your screen can only be seen from directly in front, can keep others from snooping over your shoulder.

✓ When using the Internet off campus, you should:...

Selected Answer:	✓ D. ...use padlocked or password-protected connections, and use SSLVPN when connecting to ASU servers.
Answers:	A. ...connect to ASU guest. B. ...use "free" or "open" wifi, so the state doesn't have to pay for it. C. ...send sensitive data only by email. ✓ D. ...use padlocked or password-protected connections, and use SSLVPN when connecting to ASU servers.
Response Feedback:	Correct! Use encrypted connections whenever possible - padlocked, password-protected connections, not "free" or "open." Never send sensitive information via email. Use ASU's SSLVPN (sslvpn.asu.edu) when connecting to ASU servers, on or off campus. And if you're on campus, use ASU's official wifi connection, not "asu guest" (see www.asu.edu/wifi).

Saturday, January 19, 2019 12:35:30 AM MST

← OK