

Started on Thursday, 29 September 2022, 1:22 PM

State Finished

Completed on Thursday, 29 September 2022, 1:52 PM

Time taken 29 mins 42 secs

Grade 20.00 out of 20.00 (100%)

Question **1**

Correct

Mark 1.00 out of 1.00

While there is so much focus on cyber security (and rightly so, with everyone's reliance on computers), it's also essential to implement physical safeguards, including secure office storage. What typical physical actions can someone follow to protect information throughout the day at work?

- ☒ a. Follow a clean-desk policy
- ☐ b. Dispose of prints and papers always in the bin
- ☐ c. Do not let co-workers sit too close
- ☐ d. Obscure using fake passwords stuck to your monitor



Your answer is correct.

The correct answer is: Follow a clean-desk policy

Question **2**

Correct

Mark 1.00 out of 1.00

Companies often send out reminders in the form of newsletters regarding physical (information) security. Which of the following is NOT advice you would find in such a newsletter?

- ☒ a. Check the external link in the newsletter for the latest security procedures
- ☐ b. Install lockable office drawers
- ☐ c. Hire a professional paper shredder service
- ☐ d. Install a local paper shredder in the office



Your answer is correct.

The correct answer is: Check the external link in the newsletter for the latest security procedures

Question **3**

Correct

Mark 1.00 out of 1.00

Where should you store your passwords?

- ☒ a. In a password manager
- ☐ b. Below the keyboard
- ☐ c. Behind the monitor
- ☐ d. Below the office table plate



Your answer is correct.

The correct answer is: In a password manager

Question **4**

Correct

Mark 1.00 out of 1.00

What is a good password?

- ☐ a. A password with a company name or initials in it
- ☐ b. A password that replaces letters for numbers such as 1c3br34k3r
- ☐ c. A password that adds a special character to the end such as mickeymouse!
- ☒ d. A password that is uniquely used only for one login/purpose



Your answer is correct.

The correct answer is: A password that is uniquely used only for one login/purpose

Question **5**

Correct

Mark 1.00 out of 1.00

Which of the following is NOT password hygiene advice?

- ☐ a. Store and transmit passwords securely
- ☐ b. Do not reuse passwords
- ☐ c. Choose good passwords - the longer the better
- ☒ d. A password that is hard to remember must be also a good password



Your answer is correct.

The correct answer is: A password that is hard to remember must be also a good password

Question **6**

Correct

Mark 1.00 out of 1.00

Which of the following passwords is the safest choice from the list?

- ☐ a. 123456
- ☐ b. password1
- ☐ c. George Orwell!
- ☒ d. Tomorrow is a better day ;-)



Your answer is correct.

The correct answer is: Tomorrow is a better day ;-)

Question **7**

Correct

Mark 1.00 out of 1.00

In 2021, more than 3.5M+ global users had used the password "123456 "in one of their logins, and were hacked. How long does it take an attacker to crack this password, what do you think?

- ☒ a. Below one second
- ☐ b. Around 10 seconds
- ☐ c. Around a minute
- ☐ d. Around an hour



Your answer is correct.

The correct answer is: Below one second

Question **8**

Correct

Mark 1.00 out of 1.00

What is an action that belongs to source code security?

- ☐ a. Using a password for the computer
- ☐ b. Hiring a data protection officer
- ☐ c. Store code in white font on white background when finished coding
- ☒ d. Block transfer of source code through email



Your answer is correct.


The correct answer is: Block transfer of source code through email

Question **9**

Correct

Mark 1.00 out of 1.00

In the escape room, where was there a hint regarding the use of bad source code security?

- ☐ a. The developer's GitHub provides a game shortcut
- ☒ b. The developer console in the browser shows a hidden path statement in the html code 
- ☐ c. The escape room uses weak coding principles that can be jumped simply by changing a number in the browser bar
- ☐ d. The game had a hidden Konami code implemented

Your answer is correct.


The correct answer is: The developer console in the browser shows a hidden path statement in the html code

Question **10**

Correct

Mark 1.00 out of 1.00

Which of the following items should not be disposed in your office bin?

- ☒ a. Bank account data 
- ☐ b. Gala dinner invitation
- ☐ c. An empty usb stick
- ☐ d. Sheet containing laboratory visiting hours

Your answer is correct.


The correct answer is: Bank account data

Question **11**

Correct

Mark 1.00 out of 1.00

You were working on a clinical trial project having sensitive data. After the project you received the task to get rid of the hard drive. What do you do?

- ☐ a. Delete the data and sell the hard drive on Ebay.com to cover some of your project expenses
- ☐ b. Keep the hard drive and its data at home, maybe you will have a use for the data in a future project
- ☐ c. Copy paste the data to your private computer, and throw the hard drive into the nearest collection site for electronic hardware
- ☒ d. Physically destroy the hard drive by drilling holes in it, hitting it with a hammer, magnetizing it, and finally throwing separate parts into separate fire pits 

Your answer is correct.

The correct answer is: Physically destroy the hard drive by drilling holes in it, hitting it with a hammer, magnetizing it, and finally throwing separate parts into separate fire pits

Question **12**

Correct

Mark 1.00 out of 1.00

Which was the mistake that the accountant did in the escape room?

- ☒ a. She reused the password on the sensitive file
- ☐ b. She did not protect the sensitive file with a password
- ☐ c. She had a weak password on the sensitive file
- ☐ d. There was no sensitive data appearing in the escape room



Your answer is correct.

The correct answer is: She reused the password on the sensitive file

Question **13**

Correct

Mark 1.00 out of 1.00

In the escape room, the missing employee is found through social media. What is the information security threat called where the information found on social media leads to abuse?

- ☐ a. Ghosting
- ☐ b. Quiet Quitting
- ☐ c. Blackmailing
- ☒ d. Public Oversharing



Your answer is correct.

The correct answer is: Public Oversharing

Question **14**

Correct

Mark 1.00 out of 1.00

In the escape room, the social media account of the missing employee was impersonated and abused for identity theft. What recommended action could someone take to reduce the risk of identity theft?

- ☐ a. Don't carry loyalty cards such as Starbucks Coffee in your wallet
- ☐ b. Empty your physical mailbox latest every two weeks. Avoid placing a hold on your mailbox when you are away from home for several days.
- ☐ c. Throw receipts, credit offers account statements, and expired credit cards directly in your household trash when they are no longer in use.
- ☒ d. Please don't share personal information (birthdate, AHV Number, or bank account number) because someone asks for it. ✓

Your answer is correct.

The correct answer is: Please don't share personal information (birthdate, AHV Number, or bank account number) because someone asks for it.

Question **15**

Correct

Mark 1.00 out of 1.00

Which is a typical action that is considered identity theft?

- ☐ a. Your best friend masks himself as Rocco the clown for carnaval
- ☐ b. Your neighbour accepts a parcel that is in your name from your local mail service
- ☐ c. You send a letter to your father which is signed with "Z for Zorro"
- ☒ d. You take your parents credit card to authorize for a game purchase that requires you to be 18 ✓

Your answer is correct.

The correct answer is: You take your parents credit card to authorize for a game purchase that requires you to be 18

Question **16**

Correct

Mark 1.00 out of 1.00

The following statements describe phishing as a method to trick a person. One of the statements however is not related to phishing, can you identify which one?

- ☐ a. The attack takes place via an electronic means of communication such as email or telephone.
- ☐ b. The attacker poses as a trusted person or company.
- ☐ c. The goal is to elicit confidential personal information from the victim, such as login credentials or credit card numbers.
- ☒ d. The messages include a direct or indirect call for buying a product that has well-demanded properties by men or women. ✓

Your answer is correct.

The correct answer is: The messages include a direct or indirect call for buying a product that has well-demanded properties by men or women.

Question **17**

Correct

Mark 1.00 out of 1.00

What is currently the best method to secure your online banking?

- ☐ a. Having a strong email address or account name.
- ☐ b. Having a strong password with memorable characters, upper and lower case letters, and more than eight digits.
- ☐ c. Having an email code sent to you to verify your login attempt.
- ☒ d. Having Two-Factor-Authentication enabled you to receive confirmation codes to your smartphone for every login and transaction. ✓

Your answer is correct.

The correct answer is: Having Two-Factor-Authentication enabled you to receive confirmation codes to your smartphone for every login and transaction.

Question **18**

Correct

Mark 1.00 out of 1.00

All of the following mail messages indicate a phishing attempt except one. Please identify the message with the least risk of being a phishing attempt?

- ☐ a. Dear John Doe, I have prepared your bill as a pdf. By clicking the attachment, you will find the amount and due date for the account. Kind regards, Peter
- ☐ b. Dear John Doe, during our last security check, we realized that you did not update your password in the previous 14 days. Please update your password here (link) as soon as possible. Thank you for helping us stay secure!
- ☐ c. Dear John Doe, Suzy Sorglos has sent you a LinkedIn connection request and is waiting for your response here (link). Did you know? People who stay in touch with former classmates are 25% more likely to climb the career ladder. Your LinkedIn-marketing team
- ☒ d. Dear John Doe, at our company we follow a strict security policy. We have registered suspicious behavior following one of your accounts. Please change your passwords as soon as possible and report unnatural activities. Your security team ✓

Your answer is correct.

The correct answer is: Dear John Doe, at our company we follow a strict security policy. We have registered suspicious behavior following one of your accounts. Please change your passwords as soon as possible and report unnatural activities. Your security team

Question **19**

Correct

Mark 1.00 out of 1.00

What are typical Cybersecurity challenges for a company?

- ☐ a. Constantly evolving technology
- ☐ b. Limited budget
- ☐ c. Business priorities
- ☒ d. All of the answers are correct ✓

Your answer is correct.

The correct answer is: All of the answers are correct

One of the following facts is true, do you know which one?

- ☐ a. 31% of Swiss SMEs have already fallen victim to Cyberattacks
- ☒ b. 90% of Swiss SMEs consider that it is low risk for them to get out of business due to a cyberattack
- ☐ c. 90% of Swiss SMEs rated their IT systems' continued function as very important.
- ☐ d. 100'000 SME websites worldwide are being hacked daily



Your answer is correct.

The correct answer is: 90% of Swiss SMEs consider that it is low risk for them to get out of business due to a cyberattack

[◀ Announcements](#)

Jump to...