Exam Report: 9.7.5 Practice Questions

Date: 3/25/2020 7:17:03 pm
Time Spent: 45:34

Candidate: Garsteck, Matthew
Login: mGarsteck

## Overall Performance

Your Score: 67%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

## Individual Responses

**Question 1:** Correct

You use productivity apps on your iPad tablet device while traveling between client sites. You're concerned that you may lose your iPad while on the road and want to protect the data stored on it from being compromised. Currently, your iPad uses a 4-digit PIN number for a passcode. You want to use a more complex alpha-numeric passcode. You also want all data on the device to be erased if the wrong passcode is entered more than 10 consecutive times. What should you do? (Select TWO. Each option is part of the complete solution.)

- [x] Enable the Erase Data option.
- [ ] Enable the Complex Passcode option.
- [ ] Enable the Require Passcode option.
- [x] Disable the Simple Passcode option.
- [ ] Enable the Wipe Drive option.
- [ ] Enable the Restrictions option.

### Explanation

To use a complex alpha-numeric passcode, you must disable the Simple Passcode option under Settings > General. To cause all data on the device to be erased if the wrong passcode is entered more than 10 consecutive times, you must enable the Erase Data option located in the same screen.

The Require Passcode option is enabled automatically regardless of what type of passcode you have configured. The Restrictions option is used to restrict access to specific apps. There is no Complex Passcode or Wipe Drive option on an iPad.

### References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_DEVICE_04]

**Question 2:** Incorrect

Which of the following are the BEST steps you can take to avoid having your mobile device exploited by a hacker or infected by a virus? (Select TWO).

- [ ] Turn off location services.
- [ ] Lock the screen with some form of authentication.
- [ ] Keep your device in your possession.
- [x] ~~Keep an up-to-date remote backup.~~

- [x] Keep the operating system up to date.
- [ ] Avoid anti-virus apps.

## Explanation

Keeping the operating systems up to date with the latest updates and patches will help because they often contain fixes for known security issues. Configure the screen lock to require some sort of authentication to physically access your device.

A remote backup is an essential disaster recovery solution, but will not prevent hacker exploitation or virus infection. Having your device always in your possession, it can still be hacked and infected by a virus if not protected. Anti-virus apps for Android devices will protect your device, but you should do some research to make sure you get the most effective one. Turning off locations services does not improve your device's security, and it would make it harder to find your device if you lose it.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_SEC_01]

**Question 3:** Correct

Which of the following will improve the security of sensitive information on your device if it is lost or stolen? (Select THREE.)

- [ ] Remote backup
- [x] Locator applications
- [x] A screen lock
- [ ] Keeping up to date with OS updates and patches
- [ ] Anti-malware software
- [x] Remote wipe

## Explanation

Being able to do a remote wipe of your device will keep sensitive information from falling into the wrong hands if your mobile device is lost or stolen. Having a screen lock will help keep casual users from getting access to your device, but determined hackers can find ways around a screen lock. Locator applications might help you find your device, before a determined hacker does, if you misplace it.

Keeping the operating systems up to date with the latest updates and patches will not protect your device if it falls into a determined hacker's possession. A remote backup is an essential disaster recovery solution, but will not prevent hacker exploitation or virus infection. Being up to date and having anti-malware apps for Android devices will not protect your device if it is in a determined hacker's possession.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_SEC_02]

**Question 4:** Incorrect

Applications for mobile devices fall into two categories. Some have been reviewed, approved, and signed with a certificate by the app service, and some have not.

Which category do apps fall into if they have been signed with a certificate?

Trusted

What category do apps fall into if they have not been reviewed, approved, and signed with a certificate?

Untrusted

## Explanation

Apps that have been reviewed, approved, and signed with a certificate by the app service are referred to as trusted apps.

Apps that have not been reviewed, approved, or signed with a certificate by the app service are referred to as untrusted apps. Untrusted apps might be safe, but it is risky to install them, and most devices won't allow them to be installed by default.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_SEC_03]

**Question 5:** Correct

You have an executive user who keeps sensitive information about the company on a company-owned mobile device. You want to be prepared to keep company information secure if he loses this device or if it gets stolen.

Which of the following solutions should you use? (Select TWO.)

- [ ] Mobile device management software that allows automatic detection of unfamiliar networks.
- [x] Mobile device management software that performs remote wipes.
- [x] Mobile device management software that performs full device encryption.
- [ ] Mobile device management software that automatically detects network firewalls.
- [ ] Mobile device management software that provides pop-up blocking.

## Explanation

If a mobile device with sensitive information gets lost, the best protection you can have is full encryption and the ability to remotely wipe the device's data storage.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_SEC_04]

**Question 6:** Correct

Which type of authentication would require a user fingerprint or facial recognition for a user to get past the screen lock on a mobile device and gain access to the device?

## Explanation

A biometric authentication system attempts to identify a person based on metrics, or a mathematical representation, of the subject's biological attributes, such as a fingerprint or a face recognition.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_MOBILE_SEC_05]

**Question 7:** Correct

After entering a user id and password, an online banking user must enter a PIN that was sent as a text message to the user's mobile phone.

Which of the following digital security methods is being used?

- ( ) Smart card
- (•) Multifactor authentication
- ( ) Firewall

- DLP

## Explanation

Multifactor authentication is the process of authenticating a user by validating two or more claims presented by the user, each from a different category, such as a password and the possession of a mobile phone, or a password and a fingerprint.

Data Loss Prevention (DLP) programs or devices monitors operations such as file transfers and email for user activities that could compromise data security.

A smart card could be one authentication used in multifactor authentication, but it is not a password and does not validate the possession of a mobile phone.

Firewalls are placed between the company network and the internet to filter network traffic at the IP level. They don't authenticate users.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_PREVENTION_METHODS_06]

**Question 8:** Correct

A user is choosing a method to secure a mobile device.

Which of the following types of screen locks is LEAST secure?

- Swipe lock
- Passcode lock
- Fingerprint lock
- Face lock

## Explanation

Swipe lock is the least secure of the choices presented. It is relatively easy to duplicate the swipe pattern, even as far as six feet away.

Face lock uses facial recognition that will become even more sophisticated in the future.

Passcode lock is the most common lock method and is more effective when letters are mixed with digits.

Fingerprint lock is the most secure of the choices presented.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_SECURE_MOBILE_DEVICES_01]

**Question 9:** Correct

A mobile device has poor performance and is slow to respond to screen inputs. After troubleshooting, a technician decides to perform a factory reset.

Which of the following actions should a technician take before doing so?

- Back up all data to an attached computer or a cloud backup service.
- Perform a remote wipe to clear any personal data.
- Close all running applications.
- Ensure that the battery is fully charged.

## Explanation

A factory reset will clear all data from the mobile device. To prevent the loss of this data, it should be backed up to an attached computer or a cloud backup service.

A remote wipe will clear all personal data, which will be lost if it has not been backed up.

All running applications will be closed and overwritten during a factory reset.

A factory reset can be done whether the battery is fully charged or not.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_SECURE_MOBILE_DEVICES_03]

**Question 10:** Correct

A user has configured his mobile device to unlock using facial recognition.

Which of the following methods for securing a mobile device is being used?

- An antivirus application
- A locator application
- Trusted source
- Biometric authentication

## Explanation

Facial recognition uses biometric data for authentication.

A locator application can be used to find a lost or stolen device.

An antivirus application is used to detect and remove malware.

Trusted source refers to the approved location for obtaining mobile applications, Google Play Store, App Store, and Microsoft Store.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_SECURE_MOBILE_DEVICES_04]

**Question 11:** Incorrect

A mobile device user is comparing methods for securing the device.

Which of the following methods for securing a mobile device can affect the device's performance?

- ~~Remote backup applications~~
- Full device encryption
- Locator applications
- Biometric authentication

## Explanation

Full device encryption is an effective security method for mobile devices. However, it usually requires processing resources and will slow performance.

Biometric authentication uses physical attributes such as a retinal, face, or fingerprint scan for authentication. Its drain on processing resources is minimal.

A locator application can be used to find a lost or stolen device. Its drain on processing resources is minimal.

Remote backup refers to applications that back up data on the mobile device. Usually, the backup data is stored in the cloud. While this can add a processing load, most backup applications will meter the processing so that it does not affect normal operations.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_SECURE_MOBILE_DEVICES_06]

**Question 12:** Incorrect

A technician is tasked with configuring a user's personal tablet to connect to the corporate network.
Which of the following should be performed before configuring access?

- Check that the battery is fully charged..
- Close all running apps.
- ~~Reset the tablet to factory defaults.~~
- Check the tablet for unauthorized root access.

## Explanation

Jailbreaking or rooting a mobile device weakens its built-in security and can expose sensitive data to cyber-fraud. A best practice is to deny access to a secure network to any device that has been given unauthorized root access.

Resetting the tablet to factory defaults will uninstall all apps and remove data. This is not warranted in this scenario.

Closing all running apps is not a requirement in this scenario.

Checking that the battery is fully charged is not a requirement to access a network.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_TRBLSHT_MOBILE_SECURITY_03]

**Question 13:** Correct

Joe, a user, is walking through a shopping mall. His phone frequently displays a message that additional information is needed to log in.

Which of the following is the MOST likely cause of these messages?

- Unintended Wi-Fi connections
- Leaked personal files
- Unauthorized location tracking
- Weak or dropped cellular signal

## Explanation

Many devices are configured to access any wireless connection based on signal strength by default. Secured Wi-Fi connections request additional information to log in. For better security, disable automation Wi-Fi connectivity on mobile devices.

Cellular service does not require login information. A weak or dropped cell signal is not the cause of the messages.

Leaked personal files can be the results of poor security. This is not a cause of these message.

Unauthorized location tracking may present messages, but they are not likely to ask for additional log in information.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_TRBLSHT_MOBILE_SECURITY_04]

**Question 14:** Correct

A technician suspects that data is being leaked from a tablet.

Which of the following is the BEST tool to troubleshoot this issue?

- Force stop
- Anti-malware
- Wi-Fi analyzer
- App scanner

## Explanation

An app scanner can test a mobile app for security flaws. This is the best option in this scenario.

Anti-malware can safeguard a mobile device from malware and ransomware, but typically doesn't check poorly written or poorly configured mobile apps for vulnerabilities.

A Wi-Fi analyzer can provide signal strength and signal quality information. It can be used to detect unauthorized devices on a Wi-Fi network. It is not used to check mobile apps for security flaws.

A force stop can be used to stop an application from running so that it can be uninstalled. It is not used to check mobile apps for security flaws.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_TRBLSHT_MOBILE_SECURITY_05]

**Question 15:** Incorrect

A technician suspects that an app on a tablet device may be surreptitiously using the camera without permission.

Which of the following would be the BEST way to troubleshoot this issue?

- Check the results of a cell tower analyzer.
- Run an anti-malware scan.
- Remove all Bluetooth pairings.
- ~~Perform a soft reset on the device.~~

## Explanation

An app that uses the phone camera without permission could be categorized as malware. A malware scan should detect this issue.

Removing all Bluetooth pairings will not protect the camera from being used without permission.

Checking the results of a cell tower analyzer will not prevent the camera being used without permission.

Performing a soft reset on the device will stop all apps, but will not protect the camera from being used without permission.

## References

TestOut PC Pro - 9.7 Mobile Device Security
[e_mobile_sec_pp6.exam.xml Q_MOB_DEV_SEC_TRBLSHT_MOBILE_SECURITY_06]