Cybersecurity Quiz: Answer Key

Check Your Answers and Get Your Score!

1. Which of the following would be the best password (hardest to crack)?

✓ iLm!J@c)&dl^A

Passwords that contain words that can be found in the dictionary, or contain keyboard adjacencies are very simple for hackers to crack using simple password cracking programs. Even replacing one letter here or there or using slang is very common and easily guessed. Best practice is to use a password that is at least 12 characters in length and is complex which means it contains a combination of upper and lowercase letters, numbers and special characters.

2. TRUE or FALSE: Attachments should always be treated with caution, even if you know the sender.

✓ TRUE

Attachments from an unknown source should never be opened. But attachments that appear to be from a known source can also be dangerous. If you receive an attachment that you weren't expecting or if it is not in keeping with how this contact normally communicates, best practice - even when you know the supposed sender - is to verify the legitimacy first.

3. When visiting your favorite website, a pop-up appears that reads "You have won a free Apple iPod!" What should you do?

✓ Do not click the pop-up - close it, and if possible, report it to an administrative contact on the page you were on

When an offer seems too good to be true, it is. Remember that social engineering tactics such as these are specifically designed to persuade you to react emotionally, usually out of fear or excitement.

4. Which website URL is legitimate?

✓ https://www.paypal.com/us/home

Some notable differences in the incorrect URL's are: PayPal will always use "https" because they are collecting personal information and extra security is required; anything before the forward slash is where you'll be taken, so any extra characters before the / are suspect; slight misspellings or extra characters (such as "payapl" and "pay.pal") are also red flags that you are being directed to a malicious site. They can be difficult to spot, so be sure to carefully check URL's.

5. You receive an email that says your PayPal account has been suspended pending confirmation of your personal information. The PayPal logo is in the body of the email, and the email is addressed "Dear Customer". The sender email is Service@PayPal-CustomerServiceTeam.com. What should you do?

[✓ Delete the email - it is a phishing attempt]

Spoofed emails can be difficult to spot, so it's important to look at the sender's information as well as you are addressed. As an account holder, you would most likely receive a personalized email. If you are uncertain and want to check on your account, you should contact them directly, either by phone or by logging directly into the verified site in a clean browser window.

---

6. You receive an email from a co-worker with an attachment. The subject line reads "Please See Attached Document". The email contains no further information. What should you do?

[✓ Both B&C are correct answers]

If you weren't expecting an attachment, it should always be treated with caution. Any messages that are out of sync with how the sender usually communicates are also suspect (i.e. no greeting, no details provided, etc.). If there is a question, make a call to the known contact info of the sender and confirm the validity of the message before proceeding. If you know the email is spoofed, delete it.

---

7. You receive a text message warning you that your bank account has been suspended. If says that you must click on the link in the SMS and update your credentials with the next 24 hours. Is this message safe or unsafe?

[✓ Unsafe]

Any message that attempts to create an extreme sense of urgency is suspect and therefore considered unsafe. Text messages are no exception. If you have concerns about the status of your bank account, contact the bank directly by phone or by logging into their known website in a clean browser window. Remember to always stay in control of where you land on the internet.

8. Which of the following is NOT a smart way to test a suspicious link?

[✓ Click on it]

There are safe ways to test a link without actually clicking on it. One way is to know the red flags of a malicious link, so that you are able to spot obvious attempts. But you can also hover over it, use a link expanding tool, or a link scanner.

---

9. TRUE or FALSE: Using two-factor authentication is not an effective tool for securing your accounts.

✓ FALSE

Two-factor authentication is an easy and very effective way to secure your accounts against unauthorized access. With 2FA in place, you can prevent a hacker from accessing your account even if they have cracked or stolen your password. It works by requiring a second piece of information be input - usually a pin or a code - when a login attempt is made from an unrecognized device.

---

10. What is the only true guarantee against data loss due to a cyber-attack such as ransomware?

✓ Having my data backed up and accessible

The only true guarantee you ever have against data loss is having the data backed up. While you can certainly limit your risks with good network security measures, you can't completely control the potential for human error (an employee clicking a bad link or attachment). In the case of a ransomware attack, once your system is infected, you have 2 choices - restore from backup or pay the ransom and hope that the criminals actually provide the decryption key.

---

11. Which of these is a possible cause of a data disaster?

✓ All of the above

Disaster happens! Whether it's the cause of simple human error, a weather event, faulty equipment or criminal activity the result is the same.

---

12. TRUE or FALSE: I have anti-virus protection, so when it comes to network security, I'm all set.

✓ FALSE

Anti-virus software alone is no longer enough. Network security today requires a multi-layered approach that includes firewalls, patch management, end-point protection, admin controls, end-user education and data backups management.

---

13. TRUE or FALSE: Cybersecurity is IT's responsibility. The everyday end-users in the office don't need to worry about this topic.

✓ FALSE

Cybersecurity is every employee's responsibility. Every single end-user needs to be aware of the cyber-risks that are a threat to the business because all it takes is one bad click to find yourself in the middle of an IT disaster.

---

14. TRUE or FALSE: Software and application updates are not important and can just be ignored.

✓ FALSE

Keeping your technology up-to-date is critical for overall security. Cyber-criminals routinely exploit known vulnerabilities in popular office products and online applications. When vendors issue those patches, they should be applied as soon as possible to defend against attacks targeting them.

---

15. TRUE or FALSE: Major companies like Netflix, Google, PayPal and FedEx are often the spoofed sender of phishing messages.

✓ TRUE

Hackers will often craft phishing campaigns as if they are coming from well-known, reputable brands. They can very easily spoof emails to match the look of standard messages from these companies. This is why it's so important to review the sender information, check the destination URL and to be suspicious of any message that is attempting to create a sense of urgency.

CHECK YOUR SCORE & YOUR CYBER-STATUS:

A (90-100%) - 14-15/15...You're a Cybersecurity Super Star!

B (80-89%) - 12-13/15...You Have Some Real Cyber-Savvy!

C (70-79%) - 11/15...You Know Cyber 101, But It's Time To Step Up to a Master Class

D (60-69%) - 9-10/15...Time To Up Your Cyber IQ

E (0-59%) - 0-8/15...Consider Adding Cybersecurity Training to Your To Do List

Corsica Tech is a world-class managed IT services firm, providing innovative, efficient and affordable IT security solutions for small and medium businesses. You know good IT management is important. We make IT a priority.

corsica technologies

Phone: 1.877.367.9348   E: service@corsicatech.com   www.corsicatech.com