Test Your Internet Safety IQ

Microsoft

Find out just how savvy you are about Internet safety at work and how to protect your company's (and customer's) data.

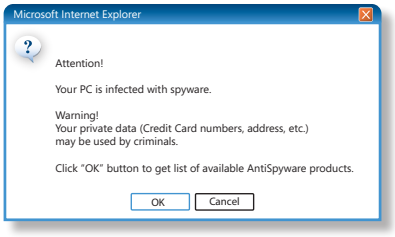
1. Which of the following is a strong password? (Check all that apply.)

- ☐ P4ssw0rds
- ☐ Ch0ckL!ck
- ☐ Your pet's name
- ☐ 011235813
- ☐ The first letters of each word in a saying, phrase, or other sentence that's easy for you to remember.

2. It's okay to share passwords with: (Check all that apply.)

- ☐ Your boss
- ☐ Your spouse
- ☐ The hotel manager
- ☐ Your coworker
- ☐ Human resources
- ☐ None of the above

3. If you see a pop-up window like this when you're on the Web, you should:



(a) Click **OK** to decide whether it's a legitimate offer.
(b) Click **Cancel**.
(c) Press **ALT + F4** to close it.
(d) Click the ☒ button.
(e) Report it to your IT department.

4. If you use public Wi-Fi (in a café or hotel, for example) that assigns you a password, your communications are secure.

(a) True
(b) False

5. How can you help protect data when you're on the road?

(a) Lock your laptop and cell phone with passwords.
(b) Don't take sensitive data away from the office. (If you must, encrypt it.)
(c) Make sure the public Wi-Fi connection encrypts data.
(d) All of the above.

6. List three signs of a fraudulent e-mail or instant message (IM):

1. _____
2. _____
3. _____

7. If you get e-mail or an IM from a manager within your organization asking for sensitive personal information (like a password or your Social Security number), it's okay to supply it.

(a) True
(b) False

8. When it comes to attachments and links in e-mail or IM, your best bet is: (Check all that apply.)

- ☐ To view every one with suspicion.
- ☐ If the message comes from someone you know personally, open or click them.
- ☐ If the message comes from a source you trust, like a company you work with regularly, open or click them.
- ☐ Don't open or click them if they're out of context–for example, *bunnies&unicorns.bmp* from your boss.
- ☐ Look at the link or attachment to decide if they're safe to click.

9. If you've installed all the security updates required by IT, you still have to worry about viruses when you click links or open attachments in e-mail messages or IM.

(a) True
(b) False

10. Which one of the following attachment extensions may contain a virus and should be viewed with suspicion?

- ☐ .exe
- ☐ .vsb
- ☐ .scr
- ☐ .pdf
- ☐ All of the above

Answers

1. Correct:
   - Ch0ckL!ck: This is a word mispronounced by a child so it's not in any dictionary; it uses upper and lower case letters, numbers, and symbols.
   - The first letters of each word in a sentence that's memorable to you–a line of a favorite poem, a popular saying, etc. It's easy for you to remember, but difficult for others to guess.

   Incorrect:
   - P4ssw0rds: Criminals won't be fooled by look-alike replacements of letters in dictionary words.
   - Your pet's name.
   - 011235813: Avoid sequences of numbers. (This is from the Fibonacci series.)
2. None of the above. Treat your passwords with as much care as the information they protect.
3. (c) Anything clickable in the pop-up window–even the Windows **Close** button ( )–can be reprogrammed to download malicious software.
4. False. The password simply means that only those with a password can access your communications. The next step is making sure that the wireless hotspot encrypts data.
5. (d)
6. Answers could include:
   - You've won a lottery you never entered. Someone will pay you a large sum of money in exchange for your help in transferring funds.
   - Misspellings, grammatical errors, weird formatting.
   - Urgent alerts from businesses you trust or from someone in your company to avoid closing your account, to verify your account, to update a database, etc.
7. False. It's possible that someone broke into the corporate network and is sending e-mail from the manager's account. To verify the legitimacy of the request, call the manager using the number on your phone or contact list, not one in the e-mail message or IM.
8. Correct:
   - View every one with suspicion.
   - Don't open or click them if they're out of context.
9. True. Someone may have broken into the corporate network and is sending e-mail from the manager's account.
10. All of the above. Any file attachment can be a vehicle for carrying a virus.