Technology Security IQ Test for Employees

Find out if your business technology is in good hands, or if your business is *at risk.*

Your employees are the number one link in making sure the security of your network and your business is strong.

Educating your employees on security best practices is the first step in protecting your business against cyber threats. This Security IQ test will help you determine if your staff is savvy on security best practices. Use this test as a spot check to determine if your employees are following proper safety protocol or if they are putting your business at risk.

Who should take this test:

☑ **CEOs and CFOs** - practicing good technology security starts at the top.

☑ **Managers** - it is the responsibility of managers to educate employees on cybersecurity best practices and why they are important.

☑ **All other employees** - anyone with access to a computer on the network should be put to the test. Employees are the key to a safe business network.

Security IQ Test

1. It is okay to share passwords with your…

a) Boss

b) Colleague

c) Friends and family

d) HR

e) None of the above

2. If you are using a public WiFi network (cafe, hotel, etc.) that assigns a password, it is okay to send confidential business data.

a) True

b) False

3. Small businesses are not targets for hackers.

a) True

b) False

4. If a stranger or a guest is walking through the office, you should…

a) Encourage a sign in, sign out, and visitor badge

b) Let them find who they are looking for

c) Escort visitors to their destination

d) A and B

e) A and C

5. What is true about passwords?

a) They should be simple and easy to remember

b) It’s okay to re-use passwords across multiple accounts

c) You must change passwords every 60 days

d) They should be complex, 8-10 characters

6. Name 3 indicators of an email phishing scheme.

a) ____________________

b) ____________________

c) ____________________

7. What should you always do when getting up from working on your computer when you leave your desk?

a) Leave it as is

b) Lock it

c) Shut it down

e) Turn it off

8. What is the weakest link in the chain when it comes to securing computers?

a) Viruses

b) Humans

c) Phishing schemes

d) Age of machine

9. What is the most common way a computer gets infected?

a) Opening an email with malware

b) Surfing the internet

c) Downloading a corrupted file

d) Installing bad software

10. It is not possible to forge a sender's email address.

a) True

b) False

11. Someone trying to infect your computer or steal your data would never call you and ask for help.

a) True

b) False

12. Macs don't need antivirus.

a) True

b) False

13. Network worms cannot spread to networks protected by a firewall.

a) True

b) False

14. Which of the following is the minimal amount of computer defense you should have in 2017?

a) Network firewalls
b) Antivirus software
c) Software security updates
d) Email spam filtering
e) Web/URL/DNS filtering
f) User security training
g) All of the above

15. There are so many security threats there is no way for a small business to keep up.

a) True
b) False

Answer & Explanation Sheet

1. e) None of the above

Do not share passwords with anyone. Even if you trust the person, passwords should always be a secret.

2. b) False

It's safer to assume that public networks are not secure. It is best not use public WiFi to enter sensitive information, send confidential data, or download software. However, if you are certain the session on the other side uses strong encryption and is validated with certificates, it is okay to transmit sensitive data.

3. b) False

43% of cyber attacks target small businesses. Cyber attacks on small businesses are growing in harm and frequency.

4. e) A & C

A visitor sign in policy ensures the safety and security of employees and and your facilities. Escorting visitors can make sure they don't enter restricted areas.

5. d) They should be complex, 8-10 characters

Complex passwords are safer and more difficult to hack. Re-using passwords puts other accounts at risk if one site is hacked. Changing passwords regularly is not always a good idea. But you should always change a password in the event of a data breach.

6. a) Indicators of a phishing scheme might include: an email address that is just slightly incorrect; asking for sensitive information; an email that is attempting to create a sense of urgency or asking you to break protocol; asking for payment; different name in the email than the from field; attachment is a zip file but you don't know the sender; something just doesn't seem right.

7. b) Lock it

Always lock your computer when getting up from your desk for any period of time.

Answer & Explanation Sheet

8. b) Humans

Humans and human error are the weakest link when it comes to securing systems.

9. b) Surfing the internet

Visiting unsecure sites is the most common, and discreet, way computers get infected.

10. b) False

A sender’s name and email address can be easily forged by masking the email or by a discrete misspelling

11. b) False

Social engineers are becoming more common. A social engineer is a person that calls posing to be an IT support desk agent, a co-worker, or other trusted source. They try baiting and phishing techniques to get sensitive information.

12. b) False

Apple’s popularity makes Macs a growing target. Reports suggest that Macs are becoming more vulnerable. Antivirus is added protection.

13. b) False

Computers can become infected while they are offsite in homes, hotel rooms, and on public WiFi connections. The infection can be brought inside the network and around the firewall after the device is returned to the office.

14. g) All of the above

Network firewalls, antivirus software, regular software security updates,email spam filtering, web/URL/DNS filtering, and user security training are all necessary steps to mitigate risk.

15. b) False

Hiring a Managed Services Provider (MSP) to control your in-house IT is a cost effective way for businesses to proactively protect their assets.

Score Sheet

14-15 correct	**Stay Secure & Safe** Great job! You are well trained on proper technology security best practices. Be sure to put them into practice everyday.
10-13 correct	**Time to Brush Up** You know some best practices, but brushing up on security best practices will make sure you know how to keep systems safe. Check your passwords and your everyday activity to make sure you aren't putting systems at risk.
9 or fewer correct	**Stop and Reassess** You might be engaging in practices that put the health of the network at risk. Train on company security policies and security best practices. Reasses in one month.

Protect Your Network From Dangerous Activity

Find out if you qualify for a business technology security audit from Pegasus Technologies.

Apply for Your Security Audit »

URL: offers.pegasustechnologies.com/business-security-audit

PEGASUS
TECHNOLOGIES

Pegasus Technologies is a Managed Services Provider focused on how people and technology work together. We build you an IT team with personalities hand picked to mach yours. When personalities work well together, technology runs more smoothly.

610.444.8256 | **info@pegasustechnologies.com** | **www.pegasustechnologies.com**