TELECO
Integrating Technologies

Who Is Your Weakest Link?

Employee Cybersecurity Quiz

What is a strong password?

a. A short password, fewer than 8 characters with no special characters.
b. A password that includes your name and birthdate.
c. A lengthy password, consisting of 12 or more characters with a mix of uppercase and lowercase letters, numbers, and special symbols.

What is two-factor authentication (2FA), and why should you enable it for your accounts?

a. A single method of authentication.
b. A method of authentication that requires two different passwords.
c. A security feature that requires users to provide two forms of identification before gaining access to an account.

What is phishing, and how can you recognize a phishing email?

a. A type of fishing sport.
b. A cyberattack where attackers impersonate legitimate entities to trick individuals into revealing sensitive information. You can recognize phishing emails by checking for suspicious email addresses, unexpected attachments, and requests for personal information.
c. A form of cyber warfare

How often should you update your passwords?

a. Regularly, ideally every 3-6 months.
b. Only when they are compromised.
c. Every few years.

What does a firewall do, and why is it important for network security?

a. A security device or software that monitors and filters incoming and outgoing network traffic. It's important for network security because it helps block unauthorized access and malicious traffic.
b. A security feature that scans your computer for viruses.
c. A device for heating a room.

What is social engineering, and how can you protect yourself from it?

a. A technique for improving your social skills.
b. A type of social gathering.
c. The art of manipulating individuals into divulging confidential information. You can protect yourself by being cautious of unsolicited requests for sensitive information and verifying the identity of requesters.

Why is it important to avoid using public Wi-Fi for sensitive tasks, such as online banking?

a. Public Wi-Fi is faster and more reliable.
b. Public Wi-Fi networks are often less secure and may be targeted by cybercriminals.
c. Public Wi-Fi is more secure than private networks.

What is malware, and how can it infect your computer or device?

a. Malicious software that can infect your computer or device. It can be delivered through email attachments, malicious downloads, or infected websites.
b. Software that improves computer performance.
c. A type of computer hardware.

If you receive a suspicious email with an attachment from an unknown sender, what should you do?

a. Open the attachment to see what it contains.
b. Forward the email to your colleagues.
c. Do not open the attachment. Delete the email or report it to your IT department.

What is the purpose of regular data backups, and how often should you perform them?

a. Backups are not necessary.
b. Regular data backups are essential for protecting against data loss due to hardware failure, cyberattacks, or other unforeseen events. They should be performed at least weekly, with critical data backed up more frequently.
c. Backups are only needed in case of a major disaster.

What is the purpose of a VPN (Virtual Private Network) in the context of cybersecurity, and how does it enhance online security?

Bonus Question

a. A VPN is used to increase internet speed.
b. A VPN helps protect your privacy and security by encrypting your internet connection and routing it through a secure server, making it difficult for hackers to intercept your data.
c. A VPN is primarily used for blocking unwanted ads and pop-ups.
d. A VPN is designed to enhance the performance of online video streaming services.

Ready to strengthen your cybersecurity? Contact Teleco, your trusted cybersecurity partner!

1218 Amber Drive • 807-345-2900 • 1-800-465-3933 • sales@teleco.ca • Teleco.ca