You receive a personal email from a famous actor asking you to visit a website to support a cause they care deeply about, stating that each ‘click’ contributes a dollar. What do you do?

Select the best answer below

A. Immediately visit the website and click the button five times because you support the cause.

B. Open the link in an incognito browser window and click to support.

C. Forward the email to five of your friends because “a celebrity contacted me!”

D. Mouse over the link in the email and realize that it looks phishy, so you click the “Report Phish” in your Outlook bar and forward it to your IT department for investigation.

E. Delete the email without opening it.
When you receive a suspicious email asking you to click links for any reason, the best course of action is to delete the email without opening it or click the “Report Phish” in your Outlook bar to report it to IT for investigation. If it smells phishy, it probably is.
Remember that when you receive a suspicious email asking you to click links for any reason, the best course of action is to delete the email without opening it or click the “Report Phish” in your Outlook bar to report it to IT for investigation. If it smells phishy, it probably is.
How can you make your password more secure?

Select the best answer below

A. Make it at least 8 characters long.

B. Use a combination of letters, numbers and characters.

C. Avoid reusing any of your passwords (make each one unique).

D. All of the above.

E. None of the above.
A secure password is unique and combines at least 8 letters, numbers and characters. And don’t use your dog’s name! For additional security, use two-factor authentication and passphrases with numbers and characters instead of passwords.
A secure password combines all of the security measures listed: it’s unique and contains at least 8 letters, numbers and characters. And don’t use your dog’s name! For additional security, use two-factor authentication and passphrases with numbers and characters instead of passwords.
A secure password is unique and combines at least 8 letters, numbers and characters. For additional security, use two-factor authentication and passphrases with numbers and characters instead of passwords.
You receive a call on your cell phone from a person claiming to be from your IT department informing you that your password has expired, and you need to set a new one. The phone number looks safe. They ask you to provide your employee number, social security number and date of birth for verification. What do you do?

A. Provide them with your information, because you want to reset your password and get back to work.

B. Ask for their contact email and phone number to verify their identity, then provide them with the information they requested.

C. Disconnect the call immediately and report it to your IT department.

D. Give them your employee number and date of birth, but keep your social security number to yourself.

E. None of the above.
Some hackers use social engineering to manipulate you into giving up sensitive information over the phone. Even if you are able to verify that they are an employee in your system, there is no guarantee that you are actually speaking with that person. You should always initiate your own password resets.
Some hackers use social engineering to manipulate you into giving up sensitive information over the phone. Even if you are able to verify that they are an employee in your system, there is no guarantee that you are actually speaking with that person. You should always initiate your own password resets.
While walking through your company’s parking lot, you see a shopping bag lying between two cars. You notice that it contains five USB drives still sealed in their original packaging – 500GB each! What do you do?

Select the best answer below

A. Open one and insert it into your PC’s USB slot, and give the other four to your co-workers.

B. Take them home and use the USB drives on your personal computer.

C. Notify building security and your IT department of the discovery and give the USB drives to them.

D. Regift the USB drives to your children for the holidays.

E. None of the above.
The “rubber ducky” attack allows a hacker to place malware in an organization using an employee as a “mule” to insert the malicious payload into the network. Never insert a USB drive or other accessory from an unknown source into ANY device that you own. And they make terrible gifts!

WELL DONE!
The “rubber ducky” attack allows a hacker to place malware in an organization using an employee as a “mule” to insert the malicious payload into the network. Never insert a USB drive or other accessory from an unknown source into ANY device that you own. And they make terrible gifts!
A salesperson comes to your office to give a presentation on some new technology that your firm is interested in acquiring. They bring the presentation in on a USB drive and ask you to insert it into your PC so that it can be projected as they narrates. What do you do?

Select the best answer below

A. Do as they ask and insert the USB drive into your PC.
B. Ask if the presentation can be downloaded instead, as your company policy prohibits the use of external USB drives, but when they can’t download it, you do ask they ask and insert the USB drive into your PC.
C. Ask them to walk through the presentation without projecting, and don’t insert the USB.
D. Ensure that they didn’t find the USB drive in a parking lot, then insert it into your PC.
E. Make extra copies of the USB drive and give one to your manager.
Unbeknownst to you, the salesperson was offered a large bribe from a hacker and the USB drive contains a ransomware payload that will lock down your systems - but by not plugging in the USB drive, and not downloading any other files, you prevented the hacker from gaining access. Whew!

WELL DONE!
Unbeknownst to you, the salesperson was offered a large bribe from a hacker and the USB drive and downloaded file both contain a ransomware payload that will lock down your systems. Avoid external USB drives and downloading files from unknown sources to personal or company PCs.
Your bank has recommended that you use two-factor authentication when you log into their site. Other websites also use this process as well to ensure user security. Which of the following is an example of two-factor authentication?

A. This one is a user name and password combination.
B. This one is password plus a CAPTCHA with a word you have to read.
C. This one is user name/password plus a CAPTCHA where you pick out the panels with sidewalks.
D. This one is user name/password plus a 6-digit code sent by text.
Two-factor authentication requires both a password and a second, different identifier - like a code sent by text, or a number generated by an app - to identify and authenticate users. This layer of security makes it much harder for hackers to gain access to your information.
Two-factor authentication requires both a password and a second, different identifier - like a code sent by text, or a number generated by an app - to identify and authenticate users. This layer of security makes it much harder for hackers to gain access to your information.
After driving to a trailhead to begin a nice afternoon of hiking, you discover that your laptop is still in your backpack, plus you have your phone (which is out of range). You need to leave your computer and phone in your vehicle but want it to be secure. What do you do?

A. Turn off all Wi-Fi.
B. Put your laptop in sleep mode.
C. Power off your devices, wrap them in a blanket and lock them securely in the trunk.
D. Wrap your devices in a thick blanket.
E. Turn off your laptop's Bluetooth.
While it is always best to keep your devices out of sight when unattended, thieves are using Bluetooth scanners to locate devices in locked vehicles - and not all devices turn off Bluetooth when ‘asleep’. Thefts often occur at trailheads where owners will be away for long periods of time - so be mindful before you take a hike.
While it is always best to keep your devices out of sight when unattended, thieves are using Bluetooth scanners to locate devices in locked vehicles - and not all devices turn off Bluetooth when ‘asleep’. Thefts often occur at trailheads where owners will be away for long periods of time - so be mindful before you take a hike.
Feeling festive, you bring in a USB powered mini-Christmas tree to decorate your office. How do you power it up?

Question 8 of 10

Select the best answer below

A. Plug it into your PC.
B. Plug it into a USB extender that connects to your PC.
C. Use a dedicated USB charger to plug the device into a regular power plug.
D. There’s no way to power it up, Christmas is canceled.
E. None of the above.
This variant of the “rubber ducky” puts malware onto lots of devices - even tiny Christmas trees! - in the hope that they end up plugged into a valuable corporate network. Never plug an unknown USB device into your PC, even if only to charge it.
This variant of the “rubber ducky” puts malware onto lots of devices - even tiny Christmas trees! - in the hope that they end up plugged into a valuable corporate network. Never plug an unknown USB device into your PC, even if only to charge it.
You’re at a cybersecurity conference in Shanghai, China, staying at a 5-star hotel. Before going out to dinner, you lock your PC to your desk and put some papers on top of it. Is your PC safe from attack and theft?

Select the best answer below

A. No, because any device left unattended can be breached.

B. Yes, because you locked it securely to the desk.

C. Yes, because the papers conceal it completely.

D. Yes, because it’s a really nice hotel.

E. Yes, because it’s not a very nice PC.
Any device left unattended can be opened and compromised through what’s generally known as the “Evil Maid” attack, where an attacker gains access by physically opening the PC to insert malware. Every device needs to be securely locked in a safe, or better yet, taken with you. Never let an unknown person have custody of your device, especially if they’re an evil maid.
Any device left unattended can be opened and compromised through what’s generally known as the “Evil Maid” attack, where an attacker gains access by physically opening the PC to insert malware. Every device needs to be securely locked in a safe, or better yet, taken with you. Never let an unknown person have custody of your device, especially if they’re an evil maid.
You get a text message from a vaguely familiar sounding name giving you a link to a Google photo album they want to share with you. You click the link and it prompts you to enter your Google credentials. What do you do?

A. Enter your credentials because you want to see the photos.
B. Immediately close the browser window and your browser.
C. Don’t click the link in the first place, delete the message and block the sender.
D. Send extra credentials because you love new photos.
E. None of the above.
This phish has been appearing more frequently, especially in social media, and the best response is to delete the text message entirely and block the sender. Closing the browser window is good if you’ve already clicked the link, but you’ve already provided the hacker with your IP address. No photo album is worth being hacked!
This phish has been appearing more frequently, especially in social media, and the best response is to delete the text message entirely and block the sender. Closing the browser window is good if you’ve already clicked the link, but you’ve already provided the hacker with your IP address. No photo album is worth being hacked!
FOR MORE INFORMATION VISIT:
Delltechnologies.com/endpointsecurity