DELL Technologies

Are you smarter than your cyber attacker?

Start Quiz

QUESTION 1 OF 14

Phishing

You receive an email from “Windows Defender Order” with an invoice that looks official for $399.99 for a Microsoft Defender Account 1-year subscription. It clearly states ‘Please don’t reply to this email’, but provides a ‘Help & Contact’ button along with a phone number. You don’t remember ordering anything like this.

What do you do?

#1

Select the Best Answer Below

A Immediately click the ‘Help & Contact’ button because you definitely don’t want this charge to hit your credit card!

B Open the email in a web browser incognito window and click the ‘Help & Contact’ button.

C Check your online credit card statement to see if the charge has hit, then use the phone number to try and discover more info.

D Inspect the email address and realize that it looks phishy, so you click the “Report Phish” through your email program and/or forward it to your IT department for investigation – and of course you do not open it!

E Delete the email without opening it.

DELL Technologies

ANSWER

Phishing

#1

WELL DONE!

Report Phish!

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.**

Next Question

DELL Technologies

ANSWER

Phishing

#1

WELL DONE, BUT...

Report Phish!

You still put yourself at risk by calling what will turn out to be a bogus phone number. One of the other options in this list is a better solution. **If it smells phishy, it probably is.**

Next Question

DELL Technologies

ANSWER

Phishing

#1

HACKED!!!

Report Phish!

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.**

Next Question

DELL Technologies

QUESTION 2 OF 14

Social Media Phishing

You check your Instagram account, and Lyle Lovett has responded directly to your comment on his posts! He asks you to connect with him via a direct message, and sends you a link to click to access very limited and valuable content.

You:

#2

Select the Best Answer Below

A Cannot believe your luck and immediately click the link.

B Copy the link and open it in an incognito window.

C Share the link on social media with your friends.

D Mouse over the link and suspect something phishy is going on, so you delete the message and block the sender.

E Block and report the sender without clicking anything.

DELL Technologies

ANSWER

Social Media Phishing

#2

WELL DONE!

Report Phish!

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.**

Next Question

DELL Technologies

ANSWER

Social Media Phishing

#2

HACKED!!!

Report Phish!

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.**

Next Question

DELL Technologies

QUESTION 3 OF 14

Password Security

Your IT department pushes you to make passwords strong – that's because these 'credentials' are among the highest value targets that attackers search for. So...

How can you make your password more secure?

#3

Select the Best Answer Below

A	Make it at least 8 characters long, and preferably longer.
B	Use a combination of letters, numbers and characters.
C	Avoid reusing any of your passwords across accounts or sites (make each one unique).
D	All of the above.
E	None of the above.

DELL Technologies

ANSWER

Password Security

#3

WELL DONE!

Use a strong password!

A secure password is unique and combines at least 8 letters, numbers and characters – and maybe even uses a unique passphrase that you remember. And don't use your dog's name! Also – be sure to use two-factor authentication – this plus a strong password provides optimal protection.

Next Question

DELL Technologies

ANSWER

Password Security

#3

WELL DONE, BUT...

Use a strong password!

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.

Next Question

DELL Technologies

ANSWER

Password Security

#3

HACKED!!!

Use a strong password!

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.

Next Question

DELL Technologies

QUESTION 4 OF 14

Social Engineering

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?

#4

Select the Best Answer Below

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.

DELL Technologies

ANSWER

Social Engineering

#4

WELL DONE!

Disconnect and contact IT!

Some attackers 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.**

Next Question

DELL Technologies

ANSWER

Social Engineering

#4

HACKED!!!

Disconnect and contact IT!

Some attackers 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.**

Next Question

DELL Technologies

QUESTION 5 OF 14

PC Infiltration

While you're taking a call, you notice some weird behavior on your screen, like the mouse moving by itself, text or console windows opening and closing, or menus flashing up and down,

So:

#5

Select the Best Answer Below

A You figure that it's a harmless PC issue and continue working.

B You check with your IT department about it, but continue working.

C You immediately stop using and shut down your PC and contact your IT department (using another device) to report the issue.

DELL Technologies

ANSWER

PC Infiltration

#5

WELL DONE!

Immediately contact IT!

Having your mouse move ‘by itself’ on the screen may indicate a serious attack involving a data breach and possible key logging. Your IT department needs to know about this asap to follow up effectively.

Next Question

DELL Technologies

ANSWER

PC Infiltration

#5

Immediately contact IT!

Abnormal behavior can indicate that an attacker is monitoring your PC, and could be both exfiltrating data and capturing keystrokes, including your passwords and other critical information. Your best option is to shut down the PC immediately and report the issue to your IT department.

Next Question

DELL Technologies

QUESTION 6 OF 14

USB-enabled Malware Attack

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?

#6

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.

DELL Technologies

ANSWER

USB-enabled Malware Attack

#6

WELL DONE!

Notify security and IT!

This type of attack allows an attacker 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!

Next Question

DELL Technologies

ANSWER

USB-enabled Malware Attack

#6

HACKED!!!

Notify security and IT!

This type of attack allows an attacker 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!

Next Question

DELL Technologies

QUESTION 7 OF 14

Ransomware

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 narrate.

What do you do?

#7

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 what 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.

DELL Technologies

ANSWER

Ransomware

#7

WELL DONE!

Don’t project or insert the USB.

Unbeknownst to you, the salesperson was offered a large bribe from an attacker 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 attacker from gaining access. Whew!

Next Question

DELL Technologies

ANSWER

Ransomware

#7

Don’t project or insert the USB.

Unbeknownst to you, the salesperson was offered a large bribe from an attacker 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.

Next Question

DELL Technologies

QUESTION 8 OF 14

Two-Factor Authentication

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 these is an example of two-factor authentication?

#8

Select the Best Answer Below

A You enter your user name and password, then are asked to input your PIN to gain access to the website.

B You enter your user name and password, plus a CAPCHA where you pick the panels which include signs.

C You enter your user name and password, and the website sends a text message to your cell phone with a one-time code which you input into the box provided on the website.

D You enter your user name, and the website requires you to input a code from a secure token which changes each minute, and is installed on your phone.

E A and C only.

F C and D only.

G None of the above.

DELL Technologies

ANSWER

Two-Factor Authentication

#8

WELL DONE!

You need both!

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 attackers to gain access to your information.

Next Question

DELL Technologies

ANSWER

Two-Factor Authentication

#8

WELL DONE, BUT...

You need both!

You're really close! There are two examples of two-factor authentication here – retry and see if you can recognize the other one.

Next Question

DELL Technologies

ANSWER

Two-Factor Authentication

#8

HACKED!!!

Oops! You need both!

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 attackers to gain access to your information. Not using it leaves you vulnerable for attackers.

Next Question

DELL Technologies

QUESTION 9 OF 14

Bluetooth Thieves

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?

#9

Select the Best Answer Below

A Turn off all Wi-Fi.

B Put your laptop in sleep mode.

C Lock your laptop and phone in the trunk.

D Wrap your laptop and phone in a thick blanket.

E Turn off your laptop and phone completely, which turns off Bluetooth.

DELL Technologies

ANSWER

Bluetooth Thieves

#9

WELL DONE!

Turn off your laptop and phone!

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 and other locations where owners will be away for long periods of time – and thieves are always watching! - so be mindful before you take a hike!

Next Question

DELL Technologies

ANSWER

Bluetooth Thieves

#9

HACKED!!!

Turn off your laptop and phone!

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!

Next Question

DELL Technologies

QUESTION 10 OF 14

USB Attack Part 2

Feeling festive, you bring in a USB-powered mini Christmas tree to decorate your office.

How do you power it up?

#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.

DELL Technologies

ANSWER

USB Attack Part 2

#10

WELL DONE!

Use a dedicated USB charger!

This variant of a USB-based attack puts malware onto lots of devices - even tiny Christmas trees! - in hopes 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.

Next Question

DELL Technologies

ANSWER

USB Attack Part 2

#10

HACKED!!!

Use a dedicated USB charger!

This variant of a USB-based attack puts malware onto lots of devices - even tiny Christmas trees! - in hopes 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.

Next Question

DELL Technologies

QUESTION 11 OF 14

Evil Maid

You're at a cybersecurity conference in Shanghai, China, staying at a 5-star hotel. Before going out to dinner, you lock your PC in the safe in your room.

Is your PC safe from attack and theft?

#11

Select the Best Answer Below

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

B Yes, because you locked it securely in the safe.

C Yes, because you also hung clothes in the closet to conceal the safe.

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

E Yes, because it's not a very nice PC.

DELL Technologies

ANSWER

Evil Maid

#11

WELL DONE!

No, any device can be breached!

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. A device that's not physically with you is open for attack. Also, never let an unknown person have custody of your device, especially if they're an evil maid.

Next Question

DELL Technologies

ANSWER

Evil Maid

#11

HACKED!!!

No, any device can be breached!

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. To be secure, every device needs to stay with you. Never let an unknown person have custody of your device, especially if they're an evil maid.

Next Question

DELL Technologies

QUESTION 12 OF 14

Spyware

You get a text message from a vaguely familiar number that says your daughter was in an accident and has been taken to the hospital. It provides a link for you to get into immediate touch.

You:

#12

Select the Best Answer Below

A	Immediately click the link because you're concerned about your daughter.
B	Do a look up of the number, discover that it's from the area where your daughter was and then click the link.
C	Don't click the link and instead text your daughter to make sure she's alright.
D	None of the above.

DELL Technologies

ANSWER

Spyware

#12

WELL DONE!

Don’t click on the link!

This type of attack is an attempt to place spyware on your phone, which can compromise your phone and potentially spread to the corporate network. You recognized that it didn’t seem ‘right’ and used another method to verify that your daughter was ok. Good job!

Next Question

DELL Technologies

ANSWER

Spyware

#12

HACKED!!!

Don’t click on the link!

This type of attack is an attempt to place spyware on your phone, which can compromise your phone and potentially spread to the corporate network. Clicking the link delivers a spyware payload to your device. Just say no to stray texts, regardless of how compelling they might be.

Next Question

DELL Technologies

QUESTION 13 OF 14

Endpoint Security

Threat actors (you might even call them hackers with malicious intent) are targeting endpoints.

Endpoints are defined as:

#13

Select the Best Answer Below

A	Desktops.
B	Desktops and notebooks.
C	Desktops, notebooks and servers.
D	Desktops, notebooks, servers, the cloud and more.
E	Desktops, notebooks, servers, the cloud and the last destination on my GPS.

DELL Technologies

ANSWER

Endpoint Security

#13

WELL DONE!

Any remotely connected device!

An endpoint is any device that is remotely connected to a network. Endpoint security is vital to protect the devices and data in your organization - so make sure you stay ahead of attackers!

Next Question

DELL Technologies

ANSWER

Endpoint Security

#13

WELL DONE, BUT...

Any remotely connected device!

An endpoint is any device that is remotely connected to a network. Endpoint security is vital to protect the devices and data in your organization - so make sure you stay ahead of attackers!

Next Question

DELL Technologies

ANSWER

Endpoint Security

#13

HACKED!!!

Any remotely connected device!

An endpoint is any device that is remotely connected to a network. Endpoint security is vital to protect the devices and data in your organization - so make sure you stay ahead of attackers!

Next Question

DELL Technologies

QUESTION 14 OF 14

Endpoint Security Part 2

Hackers with malicious intent target endpoints like desktops, laptops, mobile phones, wireless printers, servers – anything that connects to a network.

What steps should you take to help prevent an attack?

#14

Select the Best Answer Below

A Make sure I lock - and lock up - my device whenever I'm not using it.

B Update and patch my device regularly.

C Practice good email hygiene: report suspicious emails.

D Never plug an unknown device into my endpoint.

E All of the above.

DELL Technologies

ANSWER

Endpoint Security Part 2

#14

WELL DONE!

All of the above!

You've learned how to be cyber-safe and are putting it into practice. Endpoint security is vital to protect the devices and data in your organization - so make sure you stay ahead of attackers!

Next Question

DELL Technologies

ANSWER

Endpoint Security Part 2

#14

WELL DONE, BUT...

There is more to do!

There's more than one thing you must do to protect your devices. Endpoint security is vital to protect the devices and data in your organization - so make sure you stay ahead of attackers!

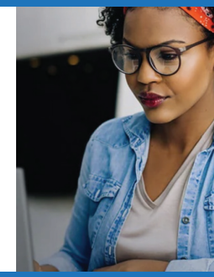
Next Question

DELL Technologies

THANK YOU!

For more information:

Visit **Dell.com/Endpoint-Security**



DELL Technologies