



RANSOMWARE, PHISHING, SMISHING, SPEAR PHISHING, SPOOFING, VISHING PHARMING

Wednesday, August 18, 2021

9 AM

Jeff Wilkinson

Sun City Summerlin Computer Club

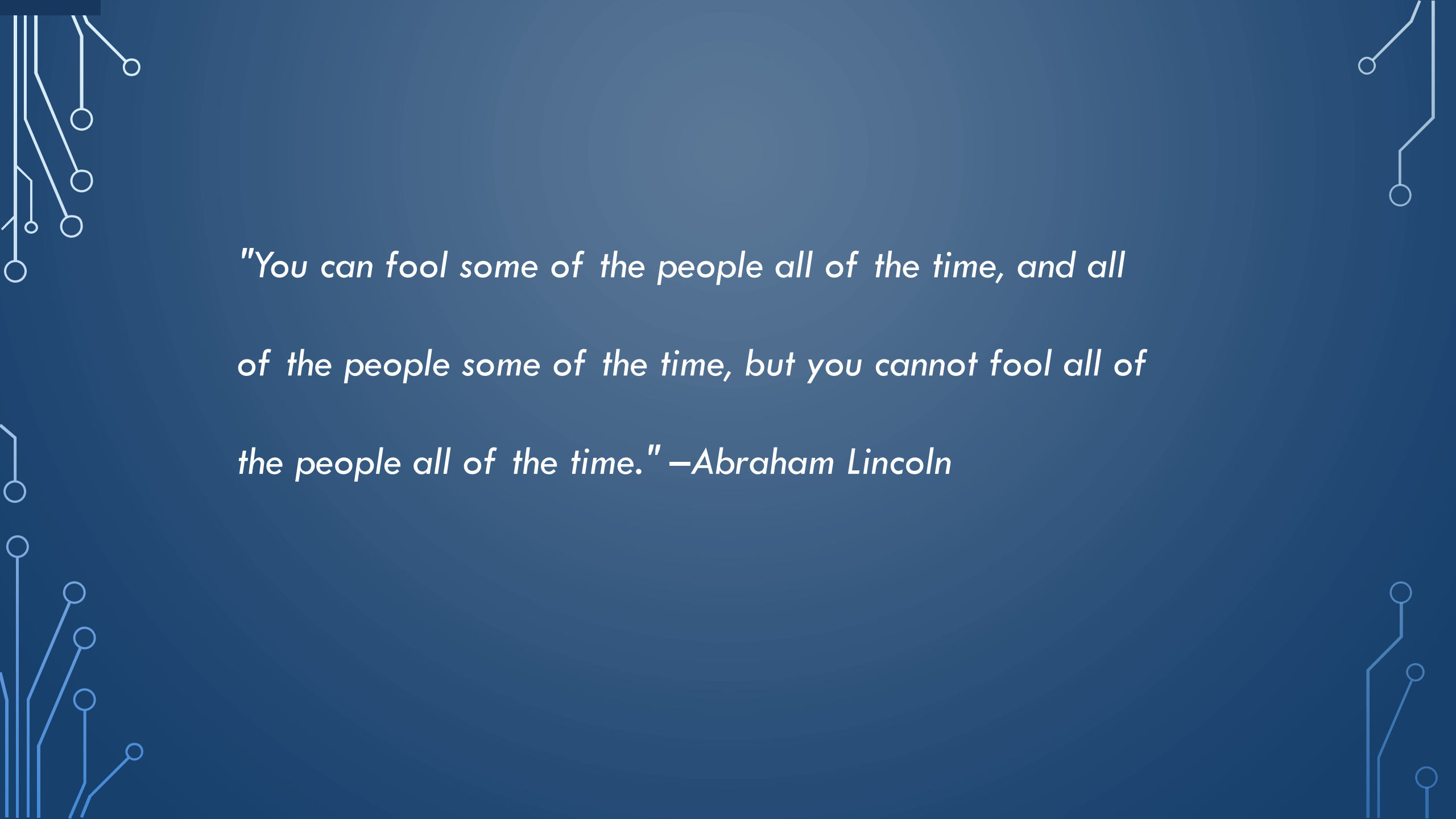
Wow!!



What does all that jargon mean??

- Ransomware
- Phishing
- Spoofing
- Review Quiz
- Questions



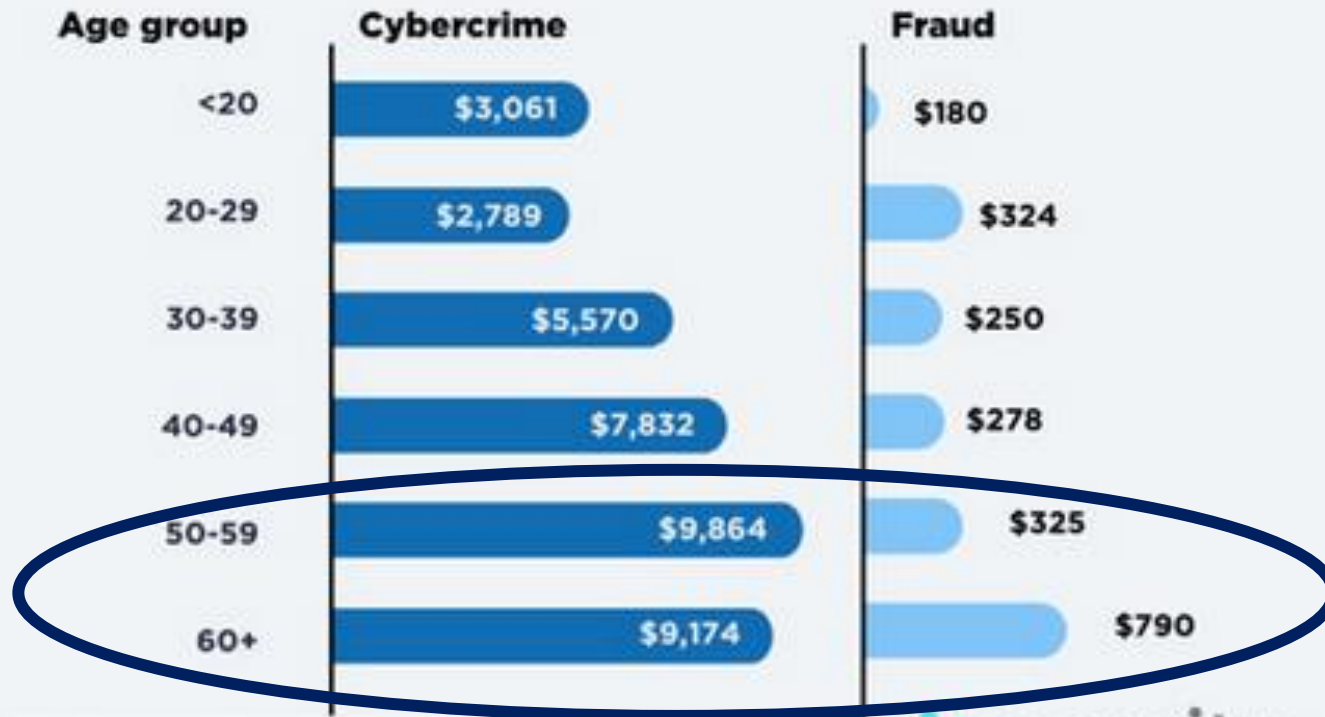
The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments and small circles, resembling a stylized PCB or network diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

"You can fool some of the people all of the time, and all of the people some of the time, but you cannot fool all of the people all of the time." –Abraham Lincoln

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight paths that branch out and terminate in small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Let us not be fooled.....

Average cybercrime and fraud loss by age group*



* Among cases in which victim's age was known and loss amount was reported

THE AVERAGE COST OF RANSOMWARE-CAUSED DOWNTIME PER INCIDENT

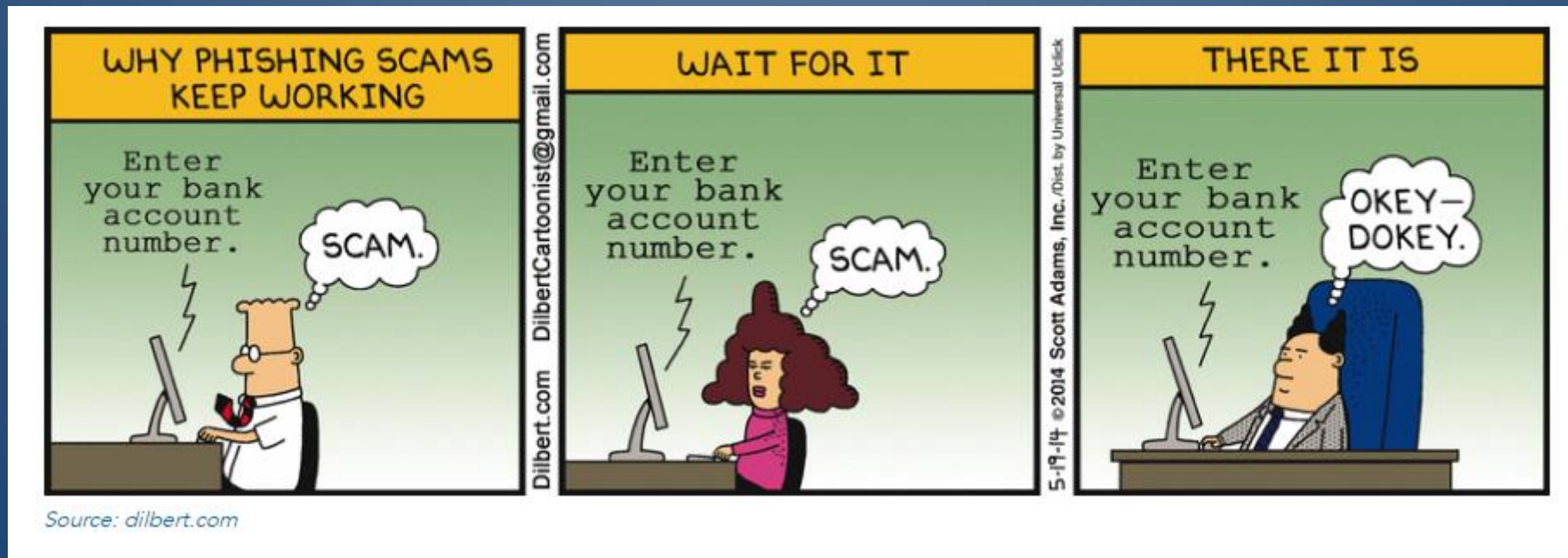


*projected

Average cost of downtime to organizations as a result of a ransomware attack, in USD.



Best defense is to be aware and exercise caution !!



Ransomware

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files and demands a ransom for their return.

Ransomware attacks can cause costly disruptions and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.



Tips for Avoiding Ransomware

The best way to avoid being exposed to ransomware or any type of malware is to be a cautious and conscientious computer user. Malware distributors have gotten increasingly savvy, and you need to be very careful about what you download or click on.

But it Happens!!

Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send \$100 worth of bitcoin to this address: QR Code

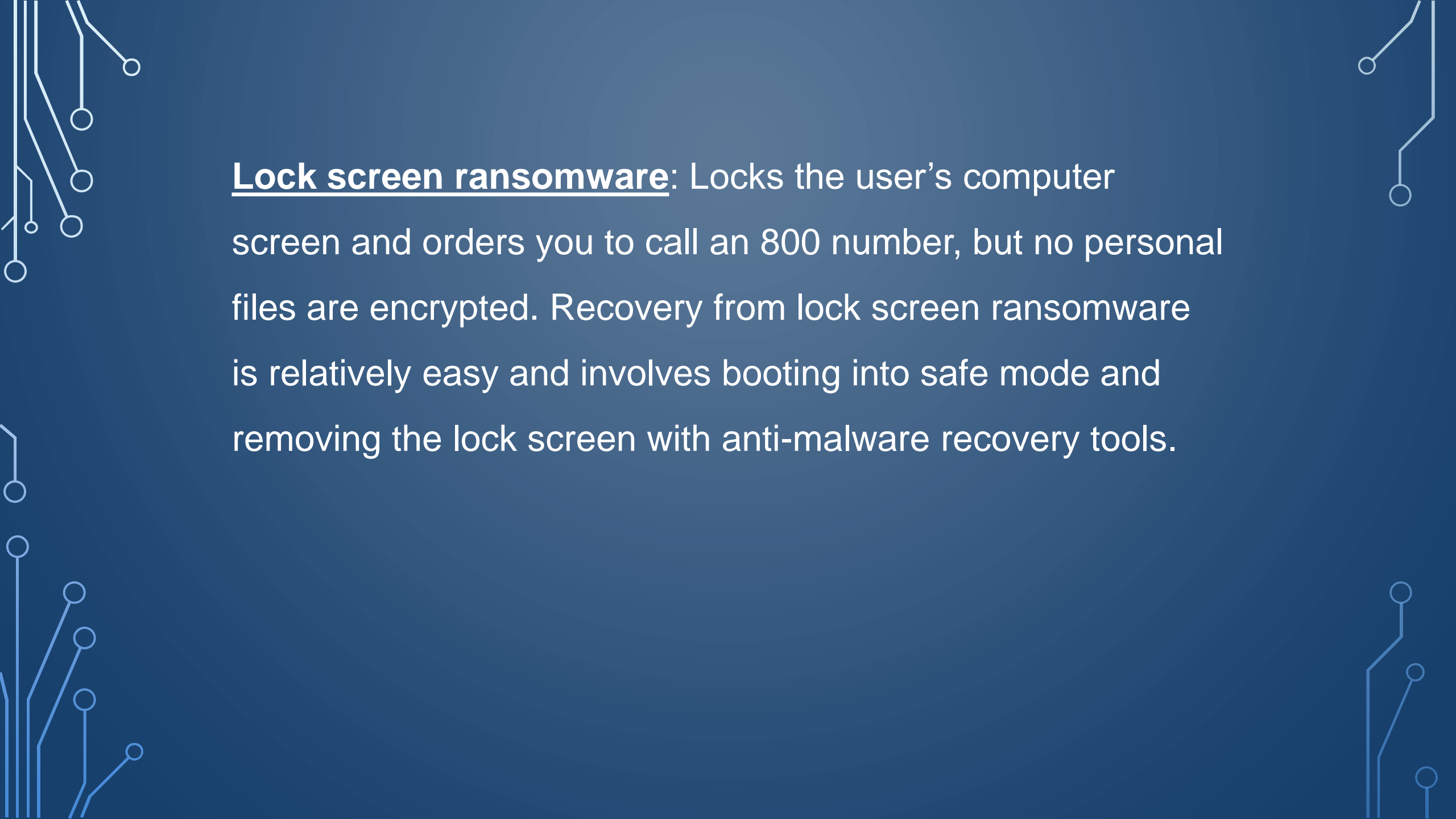
bitcoin ACCEPTED HERE

1QA9S5EmycqjzzWDc1yiWzr9jJLC8sLiY Copy

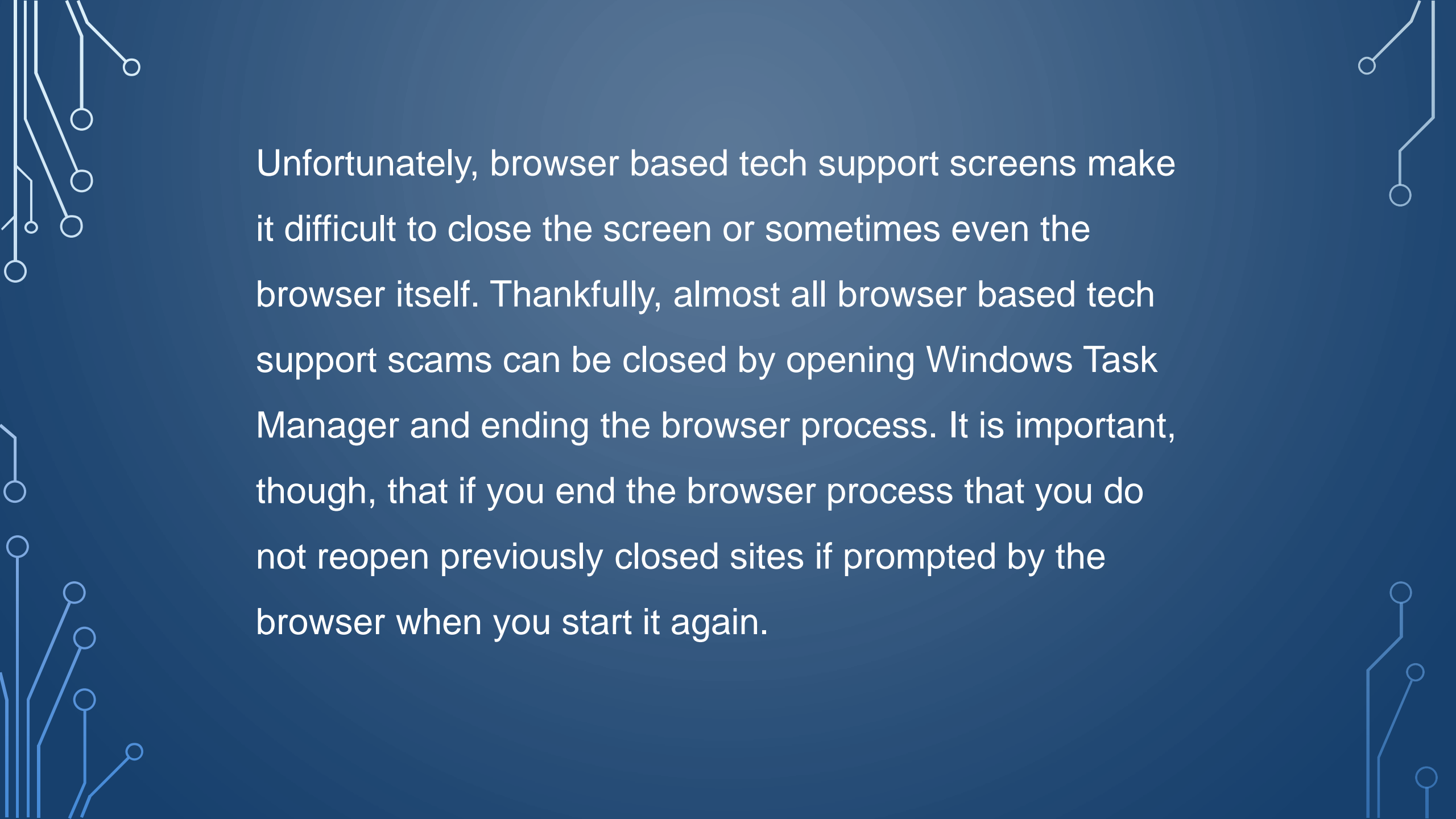
[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Check Payment **Decrypt**

- Microsoft will not call you!!
- **DO NOT** respond to calls or computer screens that ask you to call an 800 phone number
- **DO NOT** allow a third party to remotely access your machine unless you are absolutely sure of their identity and trust them

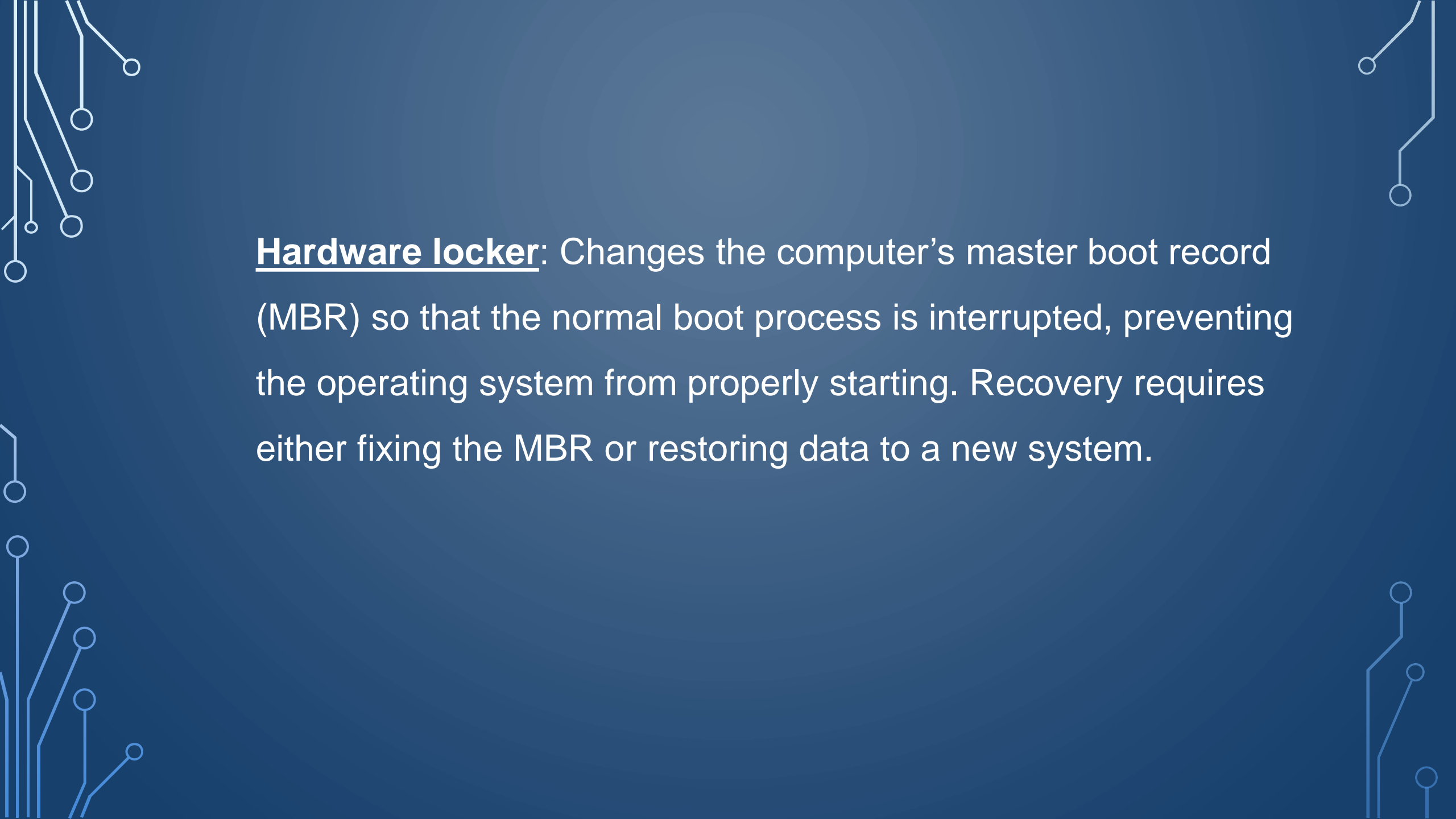
The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight paths that branch out and terminate in small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Lock screen ransomware: Locks the user's computer screen and orders you to call an 800 number, but no personal files are encrypted. Recovery from lock screen ransomware is relatively easy and involves booting into safe mode and removing the lock screen with anti-malware recovery tools.

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

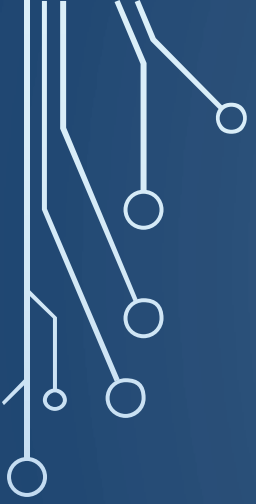



Unfortunately, browser based tech support screens make it difficult to close the screen or sometimes even the browser itself. Thankfully, almost all browser based tech support scams can be closed by opening Windows Task Manager and ending the browser process. It is important, though, that if you end the browser process that you do not reopen previously closed sites if prompted by the browser when you start it again.

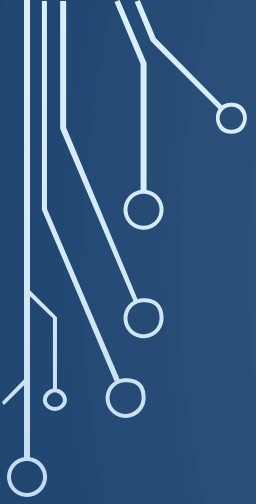



- **Encryption ransomware**: Encrypts personal files, folders, and shared network storage. The targeted files are deleted once they've been encrypted, and users generally encounter a text file with ransom payment instruction in the same folder as the newly inaccessible files.
- **Network-attached storage (NAS) ransomware**: Encrypts and/ or deletes files on a NAS system including home directories, virtual machine (VM) hypervisor backups, shadow volumes, and backup files.

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight paths that branch out and terminate in small circles, resembling a stylized PCB layout. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

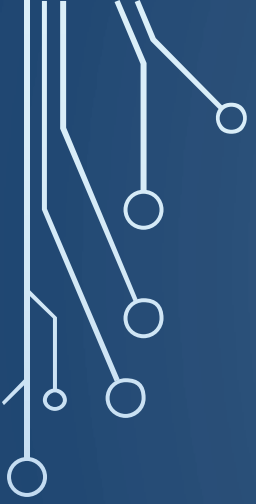



Hardware locker: Changes the computer's master boot record (MBR) so that the normal boot process is interrupted, preventing the operating system from properly starting. Recovery requires either fixing the MBR or restoring data to a new system.

- Don't open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive

- 
- 
- **Don't** open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive
 - Keep your operating system and applications up to date
- 
- 

- 
- 
- **Don't** open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive
 - Keep your operating system and applications up to date
 - Have a backup plan for important files and pictures
- 
- 

- **Don't** open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive
- Keep your operating system and applications up to date
- Have a backup plan for important files and pictures
- Use strong, unique passwords – password manager

- 
- 
- 
- 
- **Don't** open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive
 - Keep your operating system and applications up to date
 - Have a backup plan for important files and pictures
 - Use strong, unique passwords – password manager
 - Use two factor authentication for important sites

- **Don't** open attachments from unknown sources
 - Attachments from known sources should be something you expected to receive
- Keep your operating system and applications up to date
- Have a backup plan for important files and pictures
- Use strong, unique passwords – password manager
- Use two factor authentication for important sites
- Consider turning off *password save* feature in browsers

If you are a victim of ransomware:

- Contact your local FBI field office to request assistance

Las Vegas Nevada FBI Office

700 East Charleston Boulevard

Las Vegas, Nevada, 89104

Phone

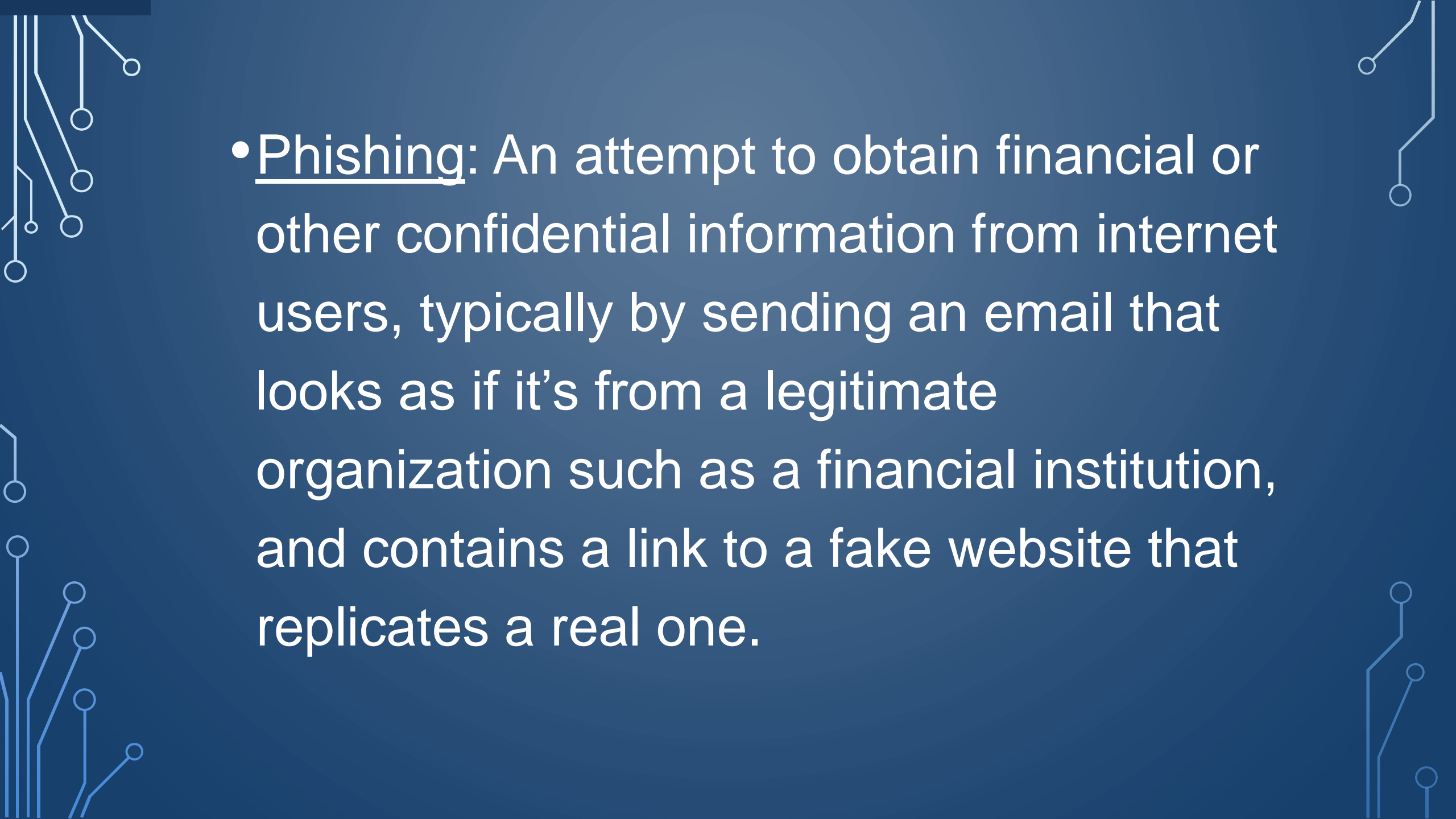
702-385-1281

- File a report with the FBI's Internet Crime Complaint Center (IC3).

Phishing



Don't Get Hooked!

- 
- The slide features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.
- Phishing: An attempt to obtain financial or other confidential information from internet users, typically by sending an email that looks as if it's from a legitimate organization such as a financial institution, and contains a link to a fake website that replicates a real one.

Who sends these phishing emails

- Hackers
- Spammers
- Criminals

A man who used **phishing** techniques to steal millions of dollars in a global business **email** compromise scheme received a 10-year prison term for his crimes.

<https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing>

Spam / phishing emails

67%

Lack of cyber security training

36%

Weak passwords / access management

30%

Poor user practices / gullibility

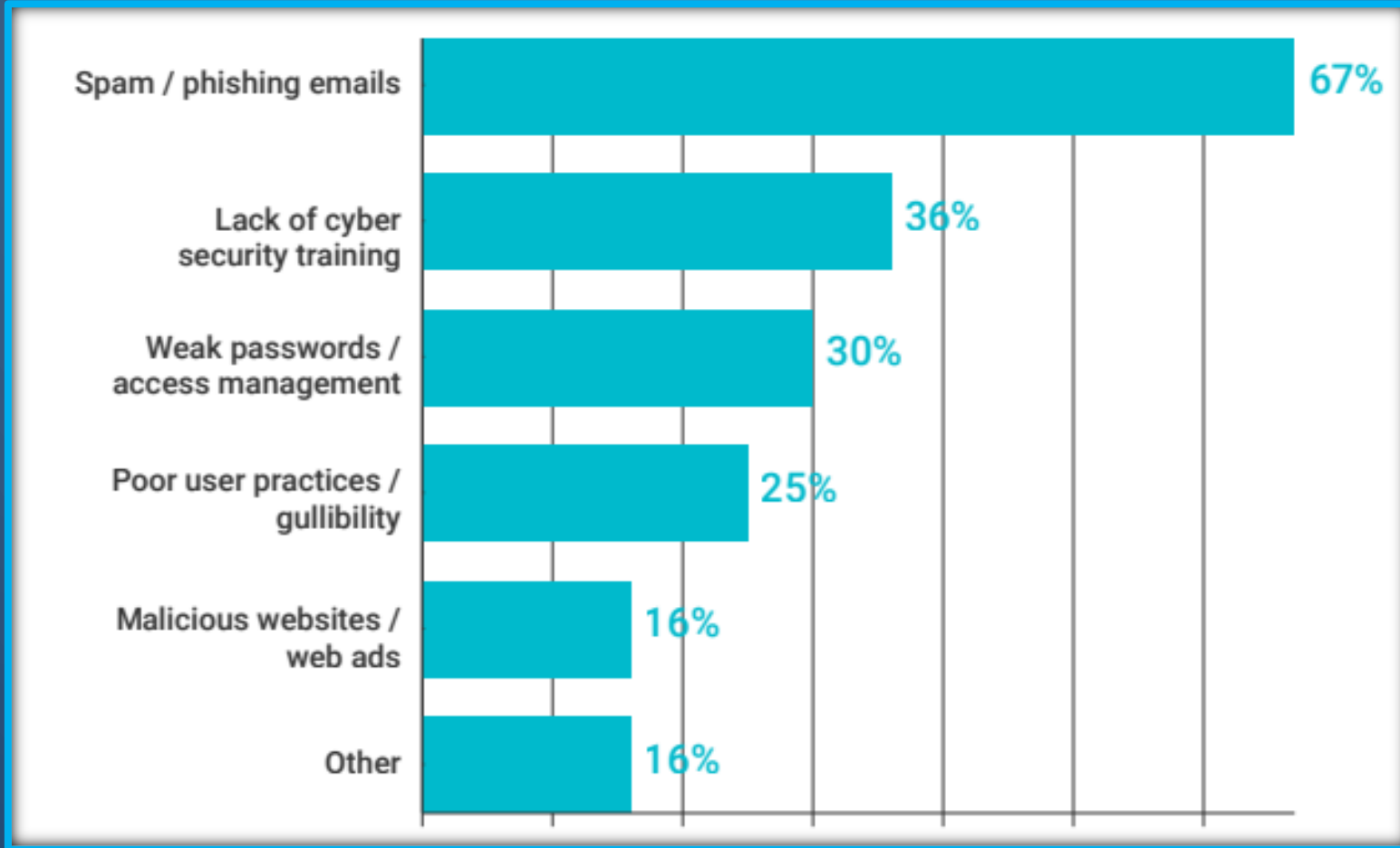
25%

Malicious websites / web ads

16%

Other

16%



Link Based Phishing Schemes

Some legitimate services such as Office 365, Google Drive, One Drive, and other well-trusted services generate their own URLs that link to hosted content.

<https://drive.google.com/drive/folders/1vAnYY1qAnp6POpATNeESfljHmgaaV-T8?usp=sharing>

This is a legitimate link – examine sender before clicking this link!!

If you don't know who sent a link such as the one above use extreme caution!!

You receive an email that looks legitimate and contains links or a form that asks you to provide personal or financial information


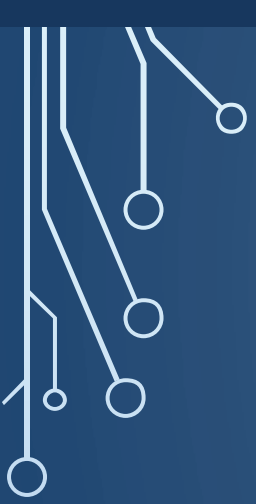


- Confirm you password



You receive an email that looks legitimate and contains links or a form that asks you to provide personal or financial information



- Ask to Confirm your password
- Informs You've been hacked, re enter personal information





You receive an email that looks legitimate and contains links or a form that asks you to provide personal or financial information

- Confirm your password
 - Informs You've been hacked, re enter personal information
 - Tells you to click on link to update your information
- 
- 



Don't Do It if you are not sure

Viruses, Malware and locking software happens almost instantly and you don't get a second chance



Some Recent “link based” Phishing schemes

- Vacation contract rental

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder
- Spotify password update prompt

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder
- Spotify password update prompt
- Promissory note

Some Recent “link based” Phishing schemes

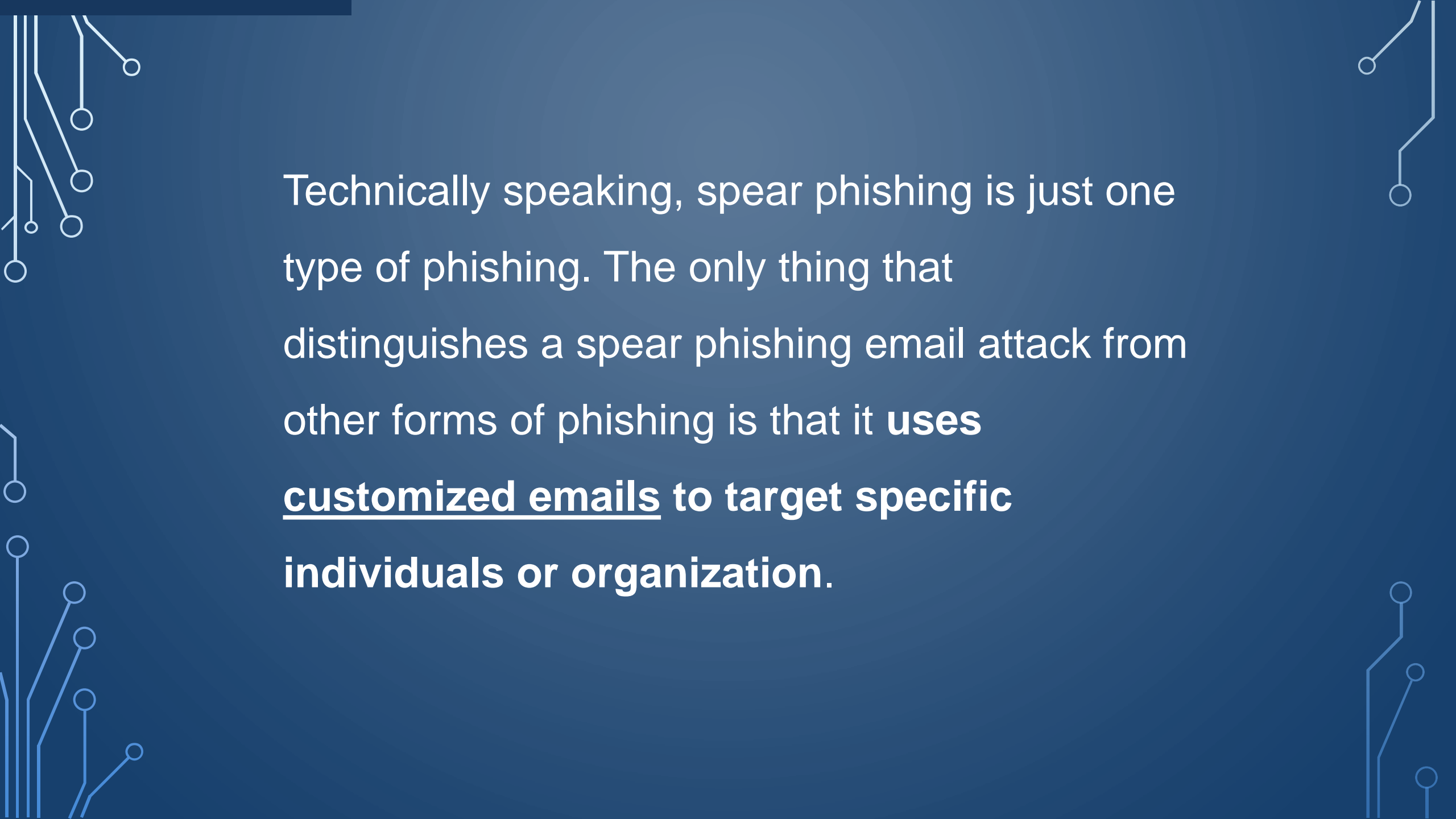
- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder
- Spotify password update prompt
- Promissory note
- Coronavirus mask availability and payment

Some Recent “link based” Phishing schemes

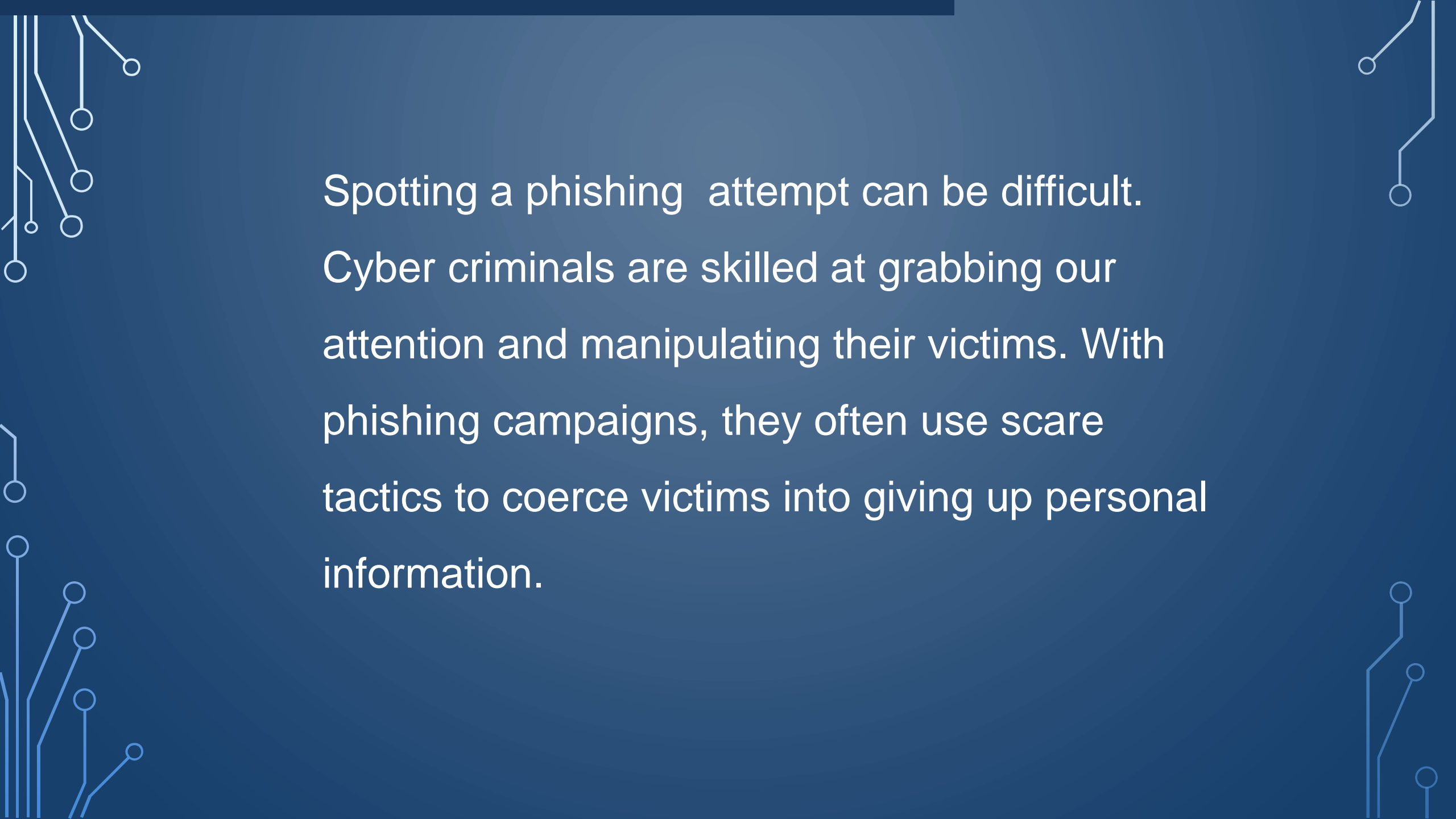
- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder
- Spotify password update prompt
- Promissory note
- Coronavirus mask availability and payment
- Notice of moving violation

Some Recent “link based” Phishing schemes

- Vacation contract rental
- Free month of Netflix streaming
- Starbucks pumpkin spice season
- Advanced ticket sales for a sold out event
- Overdue invoice reminder
- Spotify password update prompt
- Promissory note
- Coronavirus mask availability and payment
- Notice of moving violation
- Countless others that attempt to lure into performing an action

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Technically speaking, spear phishing is just one type of phishing. The only thing that distinguishes a spear phishing email attack from other forms of phishing is that it **uses customized emails to target specific individuals or organization.**

The background is a solid dark blue color. In the four corners, there are decorative white line-art elements that resemble circuit traces or network diagrams. These elements consist of thin white lines that branch out and terminate in small white circles, creating a sense of connectivity and technology.

Spotting a phishing attempt can be difficult. Cyber criminals are skilled at grabbing our attention and manipulating their victims. With phishing campaigns, they often use scare tactics to coerce victims into giving up personal information.

#1 – Misspelling Domains

Seems too easy, but this is one of the most common ways cybercriminals sneak past us in phishing scams. Take a look at the URLs below and see how long it takes you to spot what's wrong with them.

1. www.execuctech.com

2. www.rnsnbc.com

3. www.facebo0k.com

4. www.linkedin.com

1. www.execuctech.com \neq www.executech.com

1. Letter Scramble

When letters are scrambled inside longer words, our brains typically make the correction without us noticing.



NOT EVERYONE CAN READ THIS

fi yuo cna raed tihs, yuo hvae a sgtrane mnid too.
I cdnuolt blveiee taht I cluod aulacilty uesdnatnrd
waht I was rdanieg. The phaonmneal pweor of the
hmuan mnid, aoccdrnig to a rscheearch at
Cmabrigde Uinervtisy, it dseno't mtaetr in waht oerdr
the ltteres in a wrod are, the olny iproamtnt tihng is
taht the frsit and lsat ltter be in the rghit pclae. The
rset can be a taotl mses and you can sitll raed it
whotuit a pboerlm. Tihs is bcuseae the huamn mnid
deos not raed ervey lteter by istlef, but the wrod as a
wlohe. Azanmig huh? Yaeh and I awlyas tghuhot
spleling was ipmorantnt! If you can raed tihs **SHARE IT**

Cna yuo raed tihs?
Olny 55 plepoe out of 100 can.



www.rnsnbc.com \neq www.msnbc.com

2. Letter Combos

This one isn't as common as the others due to the wide number of fonts used today. In this case, the "r" and the "n" look a lot like the letter "m"

www.facebo0k.com \neq www.facebook.com

3. Number Swap

No doubt the “o” vs. “0” issue has caused problems for you in some way before. It’s also a classic method used to mask a shady URL.

www.linkedn.com

≠


www.linkedin.com

4. Missing Letters

This one doesn't work on a number of well-known URLs, but for some longer domains, it can be very tricky to spot.

This phishing email appears to have been sent by a trusted contact (i.e. friend or co-worker) or institution (i.e. bank) and might contain names, reference dates, and other items – things that only the target and the supposed sender would have knowledge of. This is all in a bid to gain their trust and make it easier to trick the target. Once they are fooled into a false sense of security, they are more likely to click on the attached link or divulge the information the attackers want.

From: Bank of America <crvdqi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdqi@comcast.net

Bank of America 

Online Banking Alert
Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at <https://www.bankofamerica.com>
to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

http://bit.do/ghsdfhgds

If you do not contact us, certain limitations may be placed on your debit card.
Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.



From: Bank of America <crvdgi@comcast.net>

Subject: Notification Irregular Activity

Date: September 23, 2014 3:44:42 PM PDT

To: Undisclosed recipients: ;

Reply-To: crvdgi@comcast.net

Bank of America



Online Banking Alert

Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.

For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at <https://www.bankofamerica.com>

to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

<http://bit.do/ghsdfhgds>

If you do not contact us, certain limitations may be placed on your debit card.

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.



bit.do

Updated 1 second ago

Domain Information

Domain: bit.do
Registrar: Registrar NIC .DO (midominio.do)
Registered On: 2011-12-04
Expires On: 2021-12-04
Updated On: 2020-12-04
Status: ok
Name Servers: mail.inmailing.com.br
mail2.inmailing.com.br

Registrant Contact

Name: Rodrigo de Almeida Siqueira
Organization: Rodrigo de Almeida Siqueira

Administrative Contact

Name: Rodrigo de Almeida Siqueira
Organization: Rodrigo de Almeida Siqueira


Technical Contact

Name: Rodrigo de Almeida Siqueira
Organization: Rodrigo de Almeida Siqueira

.br is the top level country code for Brazil

If you unknowingly provide hackers sensitive personal information or account data they can create new user credentials or install malware (such as backdoors) into your system to steal sensitive data.

From: Costco Shipping Agent <manager@cbbcbuilding.com> Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbbcbuilding.com>




Unfortunately the delivery of your order [COS-0077945599](#) was cancelled since the specified address of the recipient was not correct. You are recommended to complete [this form](#) and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

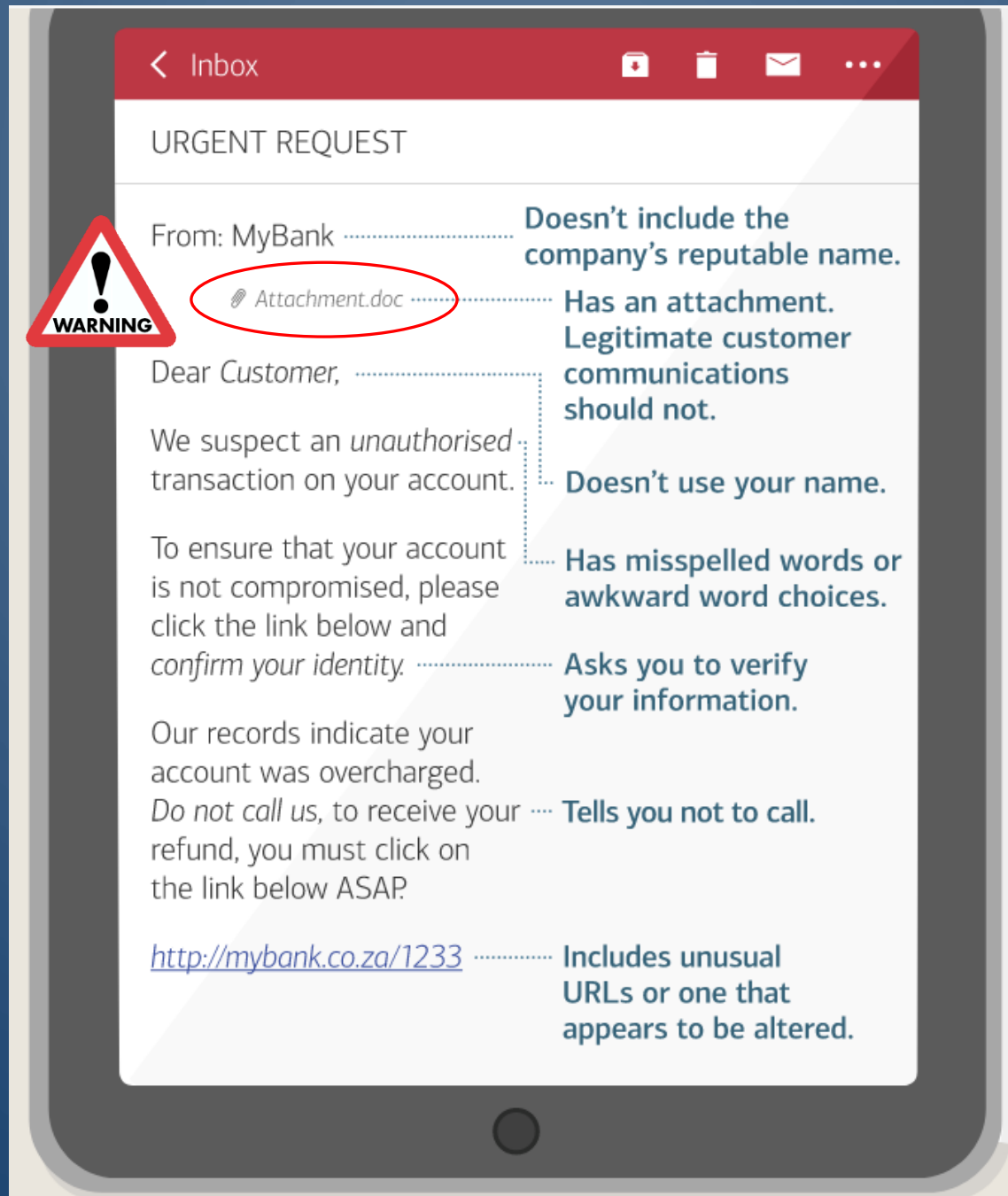
1998 - 2013
Costco Wholesale Corporation
All rights reserved

"Costco's" logo is just a bit off. This is what the Costco logo is supposed to look like.



See the difference? Subtle, no?





From Anthem <donot-reply@cerveo.com> ☆

Subject **EFT Remit Alert**

To jeff@[redacted] ☆

You've received an encrypted message from INVOICE@anthem.com

[View your message](#)

Save and open view your message (document), and follow the instructions.

Sign in using your following email address

CONFIDENTIALITY NOTICE: This e-mail, including any attachments, may contain confidential, privileged and/or proprietary information which is solely for the use of the intended recipient(s). Any review, use, disclosure, or retention by others is strictly prohibited. If you are not an intended recipient, please contact the sender and delete this e-mail, any attachments, and all copies



The screenshot shows an invoice from ACME. It includes a header with the ACME logo and a table of charges. The table has columns for 'Description', 'Quantity', 'Unit Price', and 'Amount'. The total amount is \$1,200.00.

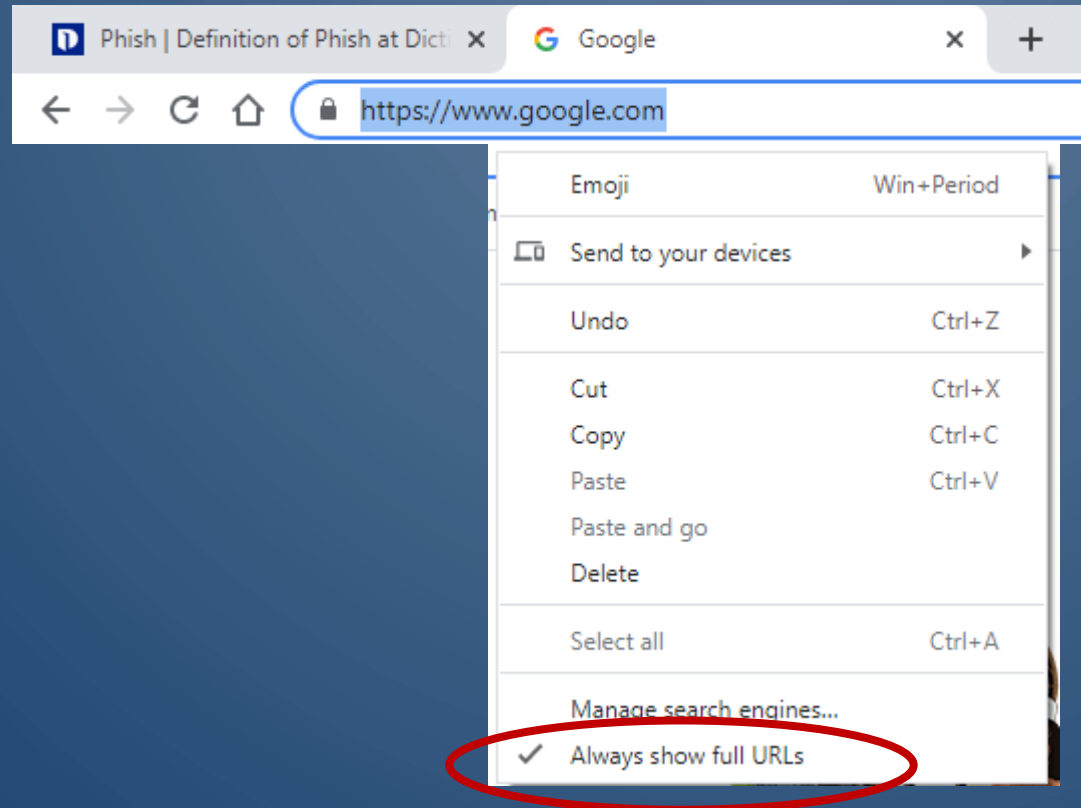
Description	Quantity	Unit Price	Amount
Service Charge	1	\$1,200.00	\$1,200.00
TOTAL			\$1,200.00



Even if a link looks legitimate it could be a phishing link in disguise – always go to the website by entering its *correct* URL directly in your browser

Criminals are registering domains that appear to look like legitimate bank domains and the fact they're fake goes unnoticed because users don't know how to spot an imposter or their email client doesn't show the full domain in the subject line.

In Google Chrome right click in search bar and check
Always show full URLs



Your **Norton** subscription has expired

Sun, 20 Jun 2021 16:46:11 -0400 (EDT)

If your PC is unprotected, it will run risk of viruses and other malware.

After the expiration date has passed, your computer becomes more susceptible for many different virus threats.

LIMITED TIME OFFER:

(80%) renewal discount Today

Name	Clarencesmith
Email	Clarencesmith@gmail.com
Discount:	(80%) renewal discount Today
LIMITED TIME OFFER:	06/21/2021

Renew Now!

<https://gghj.s3.amazonaws.com/caa.html>

amazonaws.com

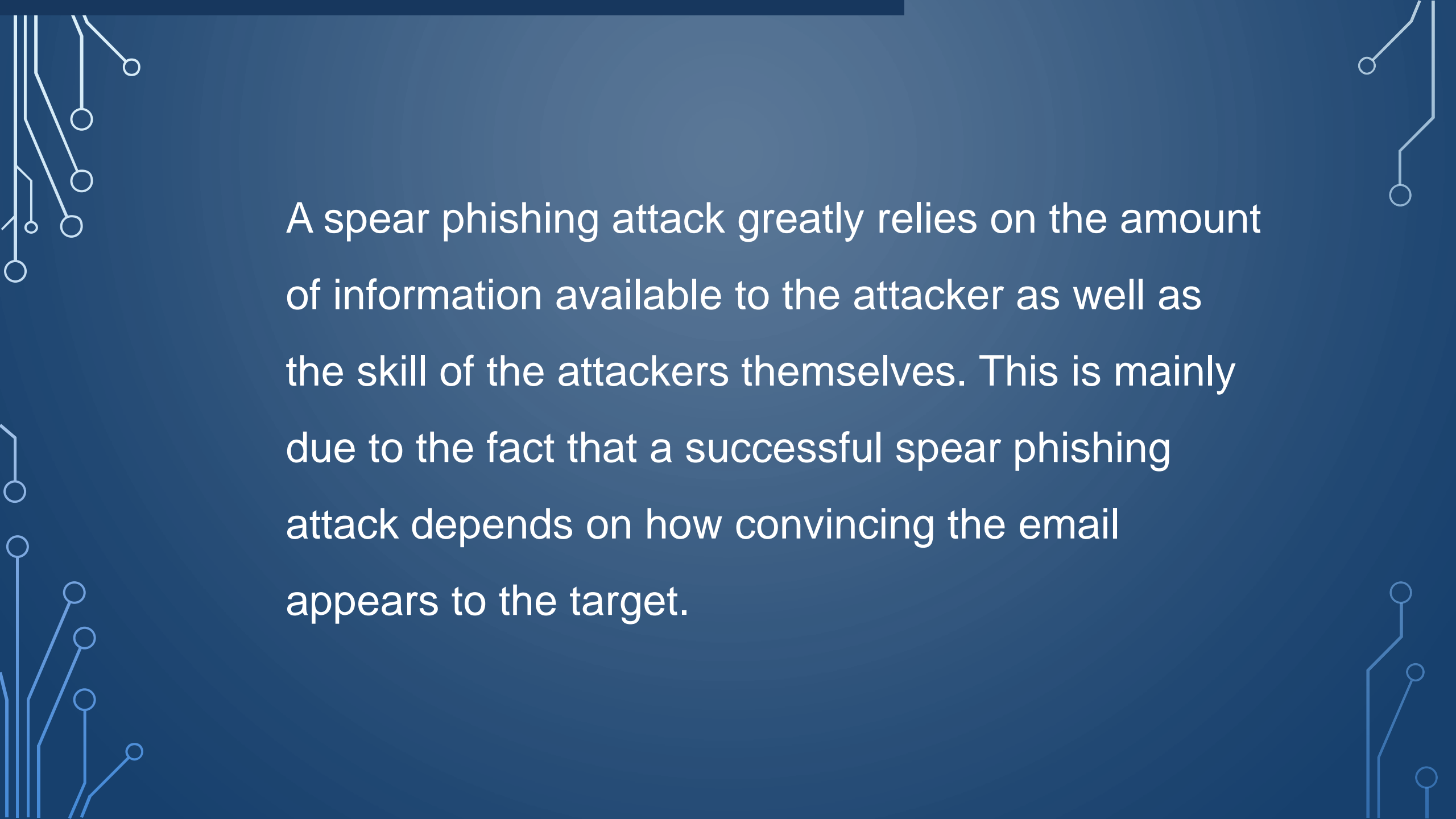
Updated 3 days ago 



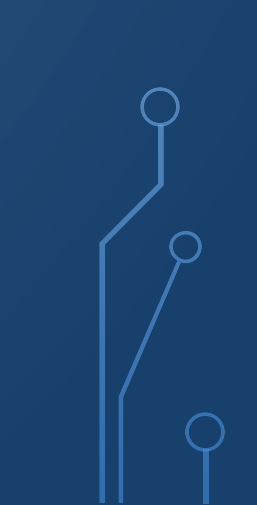


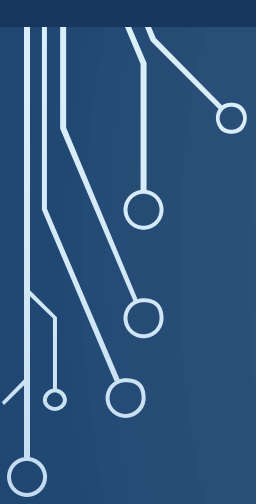
Domain Information

Domain:	amazonaws.com
Registrar:	MarkMonitor Inc.
Registered On:	2005-08-18
Expires On:	2024-01-15
Updated On:	2019-05-07
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	r1.amazonaws.com r2.amazonaws.com u1.amazonaws.com u2.amazonaws.com

WHOIS – shows
registrant of this
domain name

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

A spear phishing attack greatly relies on the amount of information available to the attacker as well as the skill of the attackers themselves. This is mainly due to the fact that a successful spear phishing attack depends on how convincing the email appears to the target.



To avoid becoming a victim of spear phishing, or any other phishing scams for that matter, good attention to detail is the key. Even the most well-made phishing emails contain minor flaws that can reveal it as a fake. Awareness of the recent phishing trends can also help to avoid falling victim to a phishing scam.

Things to watch out for:

- Urgent or Threatening Language
 - Real emergencies rarely happen over the internet
 - Threats of closing account
 - Cancel card
 - Send to collection
 - Ruin credit rating

Requests for Sensitive Information

Anyone asking for sensitive information using email or texting probably shouldn't be trusted with it anyway

- Links directing you to bogus login pages
- Requests to update account information
- Demands for financial information, even from your bank!



Offer to good to be true.....

- Winning a lottery is unlikely, winning a lottery you didn't enter is impossible
- Prizes you have to pay to receive
- An inheritance from long lost relatives

Unexpected emails

- Receipts for items you didn't purchase
- Updates on deliveries for things you didn't order

LOOK OUT FOR:

Information MisMatches



- Attachments you didn't ask for
- Weird file names
- Uncommon file types

Unprofessional Design

- Incorrect or blurry logos
- Image only emails – unable to highlight text
- Company emails with little, no, or incorrect formatting



If you spot any of these Red Flags in an email:

- **Don't** click any links
 - **Don't** reply or forward the email
 - **Don't** open any attachments
- 
- 

What Do I do if I click on a phishing email link?

The link doesn't seem to go anywhere, but you realize after the fact that this might have been a link laced with who knows what: malware, ransomware, spyware, adware, scareware?

- Ransomware
 - Ransomware is malicious software that prevents or restricts users from accessing computer systems or files until a ransom is paid. Computers typically become infected by ransomware when the user clicks on a malicious link or opens an infected attachment in an email.
 - The solution can be as easy as rebooting your computer
 - Or as complex as formatting your hard drive and reloading your software

- **Create passwords and make them strong** Half of seniors do not use the password feature on at least one of their internet-enabled devices, leaving it open to whomever may pick it up, according to research conducted by Home Instead, Inc., franchisor of the Home Instead Senior Care network. Lock all of your devices including computer, tablet and smartphone with secure passwords. That will keep prying eyes out and add a line of defense **in case your devices are lost or stolen**. A strong password is at least 12 characters long. Strong password tips include the use a mix of letters, numbers and symbols, and try not to include personal information.

We recommend using a password manager









- **Secure access to your accounts.** Since passwords can be stolen, adding two-step authentication to accounts provides a second layer of protection. Many online services, including apps and websites, offer free options that could help you protect your information and ensure it's actually you trying to access your account – not just someone with your password.
- Use cell phone number that can receive text messages to receive authentication code

- **Think before you act.** Emails and communication that create a sense of urgency such as a problem with your bank account or taxes is likely a scam. Consider reaching out directly to the company by phone to determine if the email is legitimate or not.
- **When in doubt, throw it out.** Clicking on links in emails is often how scammers get access to personal information. If an email looks unusual, even if you know the person who sent it, it's best to delete it. Remember that scammers can commandeer friends' email addresses and send you messages posing as them. Turn on spam filters for your email account to help filter suspicious messages.
- **Share with care.** Be aware of what you share publicly on social media sites like Facebook. Adjust your privacy settings to limit who can see your information. **Avoid sharing your location.**

- **Use security software.** Install security software and keep it updated.
- **Adjust your browser safety settings.** You likely search for news, information and products by using an internet browser such as Firefox, Google Chrome, Internet Explorer and Safari. Adjust your settings in each of those browsers to set your options for optimum security. Those menus can often be found in the upper right corner of your browser. Consider clearing your browsing history at the end of your session so you don't leave a trail of sensitive data.

Settings

Search settings

-  You and Google
-  Autofill
-  **Safety check**
-  Privacy and security
-  Appearance
-  Search engine
-  Default browser
-  On startup

Advanced

Extensions

About Chrome

You and Google



W Jeff

Syncing to clearmeadows11@gmail.com

Turn off

Sync and Google services

Manage your Google Account

Customize your Chrome profile

Import bookmarks and settings

Autofill



Passwords




Payment methods



Addresses and more


Settings

Search settings


 You and Google


 Autofill

 **Safety check**

 Privacy and security

 Appearance

 Search engine

 Default browser

 On startup

Advanced 

Extensions 

About Chrome

Safety check



Chrome can help keep you safe from data breaches, bad extensions, and more

[Check now](#)

Privacy and security



Clear browsing data

Clear history, cookies, cache, and more 



Cookies and other site data

Third-party cookies are blocked in Incognito mode 



Security

Safe Browsing (protection from dangerous sites) and other security settings 



Site Settings

Controls what information sites can use and show (location, camera, pop-ups, and more) 




Privacy Sandbox

Trial features are on 


Settings


Search settings

 You and Google

 Autofill


 **Safety check**

 Privacy and security

 Appearance



 Search engine


 Default browser

 On startup



Advanced 

Safety check

 Safety check ran a moment ago 

 Updates
Google Chrome is up to date

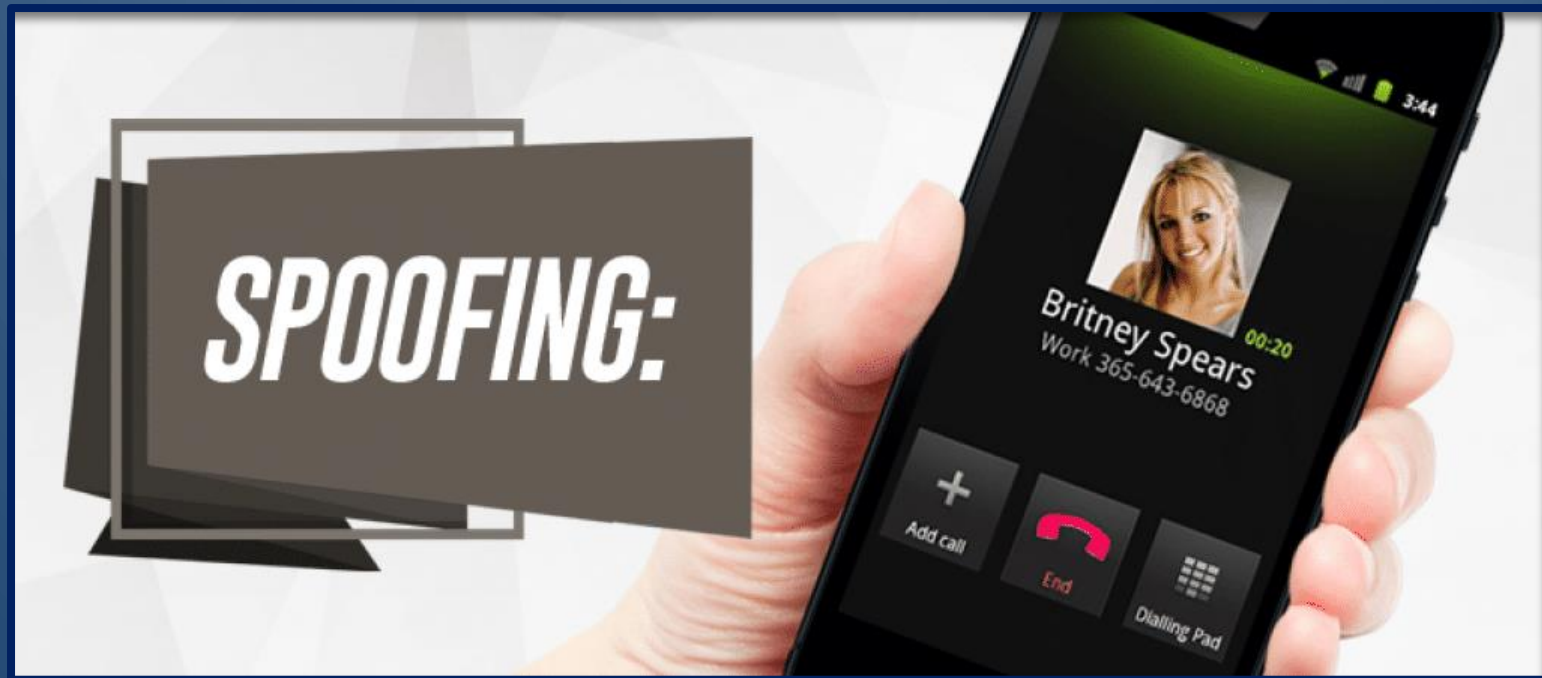
 Passwords
No compromised passwords found 

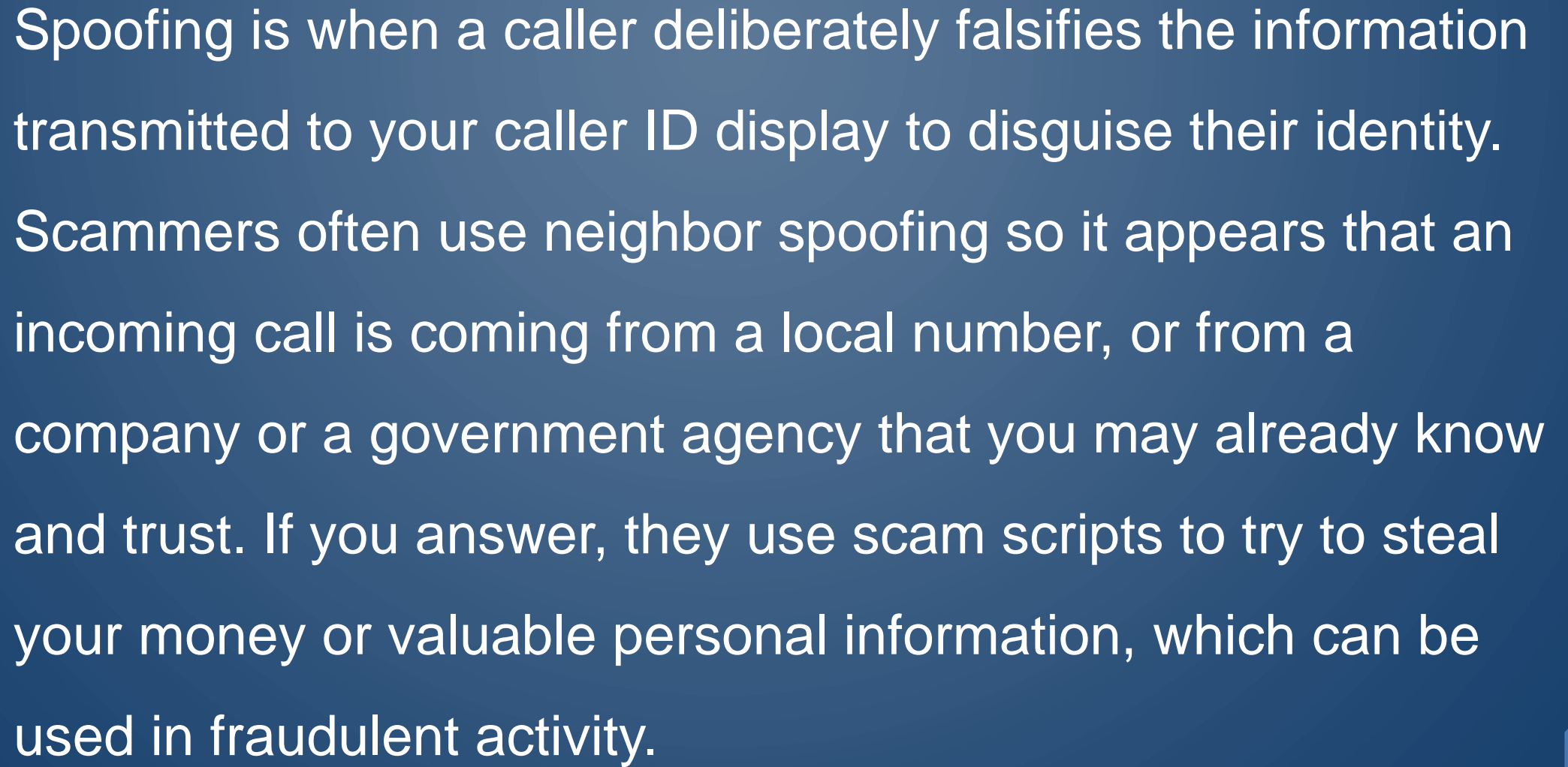
 Safe Browsing
Standard protection is on. For even more security, use enhanced protection. 

 Extensions
You're protected from potentially harmful extensions 

- **Use the default firewall security protection on your computer.** Your operating system (OS) likely has default firewall settings that will protect your computer without needing adjustment. If your antivirus software includes additional firewall protection that you can adjust separately, consider contacting a computer professional for assistance to ensure you're safely protected without over-blocking sites and programs you use regularly.

SPOOFING



The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by small circles, resembling a network or data flow diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Spoofting is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbor spoofing so it appears that an incoming call is coming from a local number, or from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

Spooftng can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Caller ID Spoofing


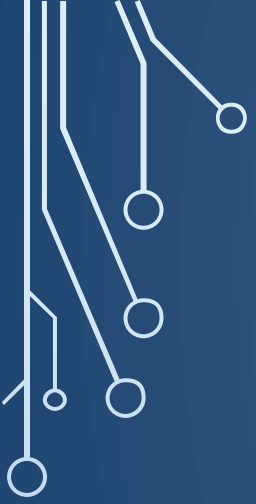
Website Spoofing

IP Spoofing

DNS Server Spoofing

VISHING





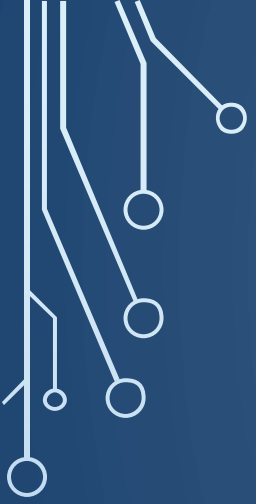





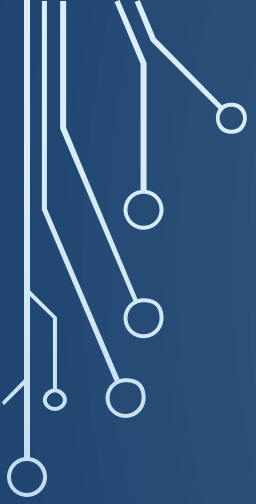



Vishing is a phone version of email phishing and uses automated voice messages to steal confidential information.

The term is a combination of "voice" and "phishing."

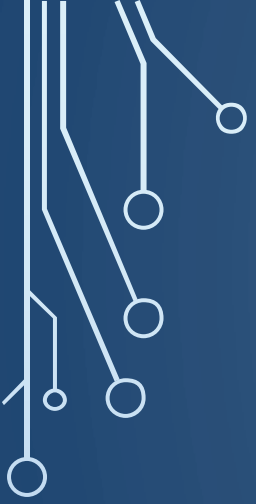



Vishing attacks use a **spoofed caller ID**, which can make the attack look like it comes from either a known number or perhaps an 800-number that might cause the user to pick up the phone. Vishing often uses VoIP technology to make the calls.

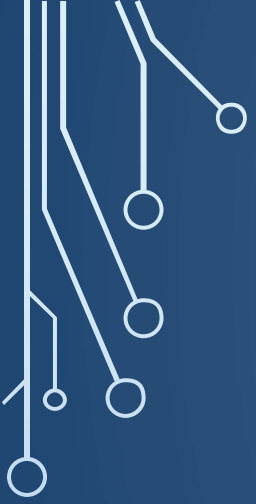



- 
- 
- You may not be able to tell right away if an incoming call is spoofed. Be extremely careful about responding to any request for personal identifying information.
- 
- 

- 
- 
- You may not be able to tell right away if an incoming call is spoofed. Be extremely careful about responding to any request for personal identifying information.
 - Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- 
- 

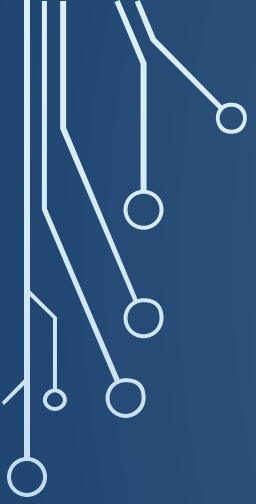



- You may not be able to tell right away if an incoming call is spoofed. Be extremely careful about responding to any request for personal identifying information.
- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.

- 
- 
- 
- 
- Do not respond to any questions, especially those that can be answered with "Yes" or "No."
 - Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.

- 
- 
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request.

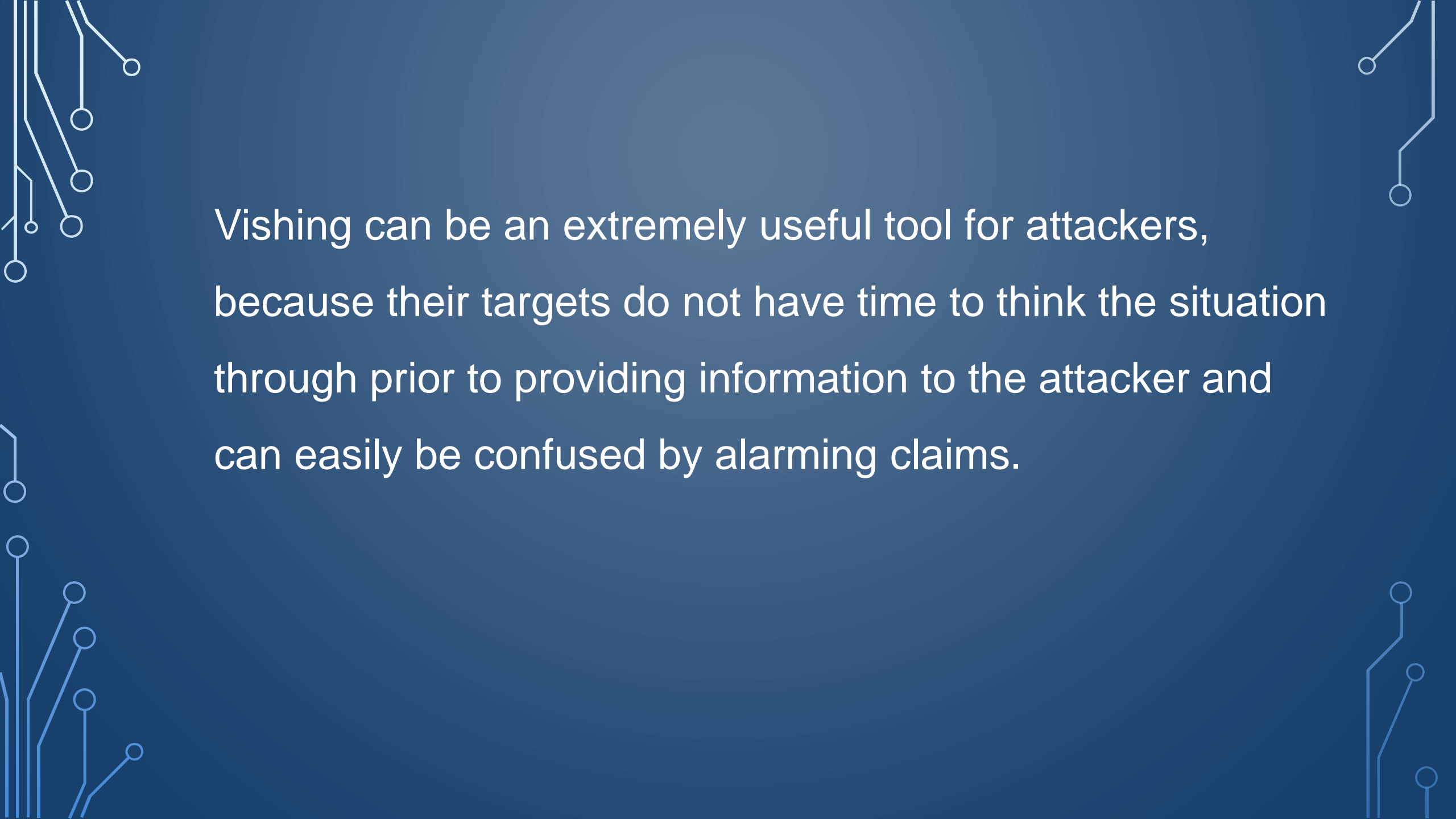
You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

- 
- 
- Use caution if you are being pressured for information immediately.

- 
- 
- 
- 
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.

- Talk to your phone company about call blocking tools and check into apps that you can download to your mobile device. The FCC allows phone companies to block robocalls by default based on reasonable analytics. More information about robocall blocking is available at [fcc.gov/robocalls](https://www.fcc.gov/robocalls).

Remember to check your voicemail periodically to make sure you aren't missing important calls and to clear out any spam calls that might fill up your allotted space.

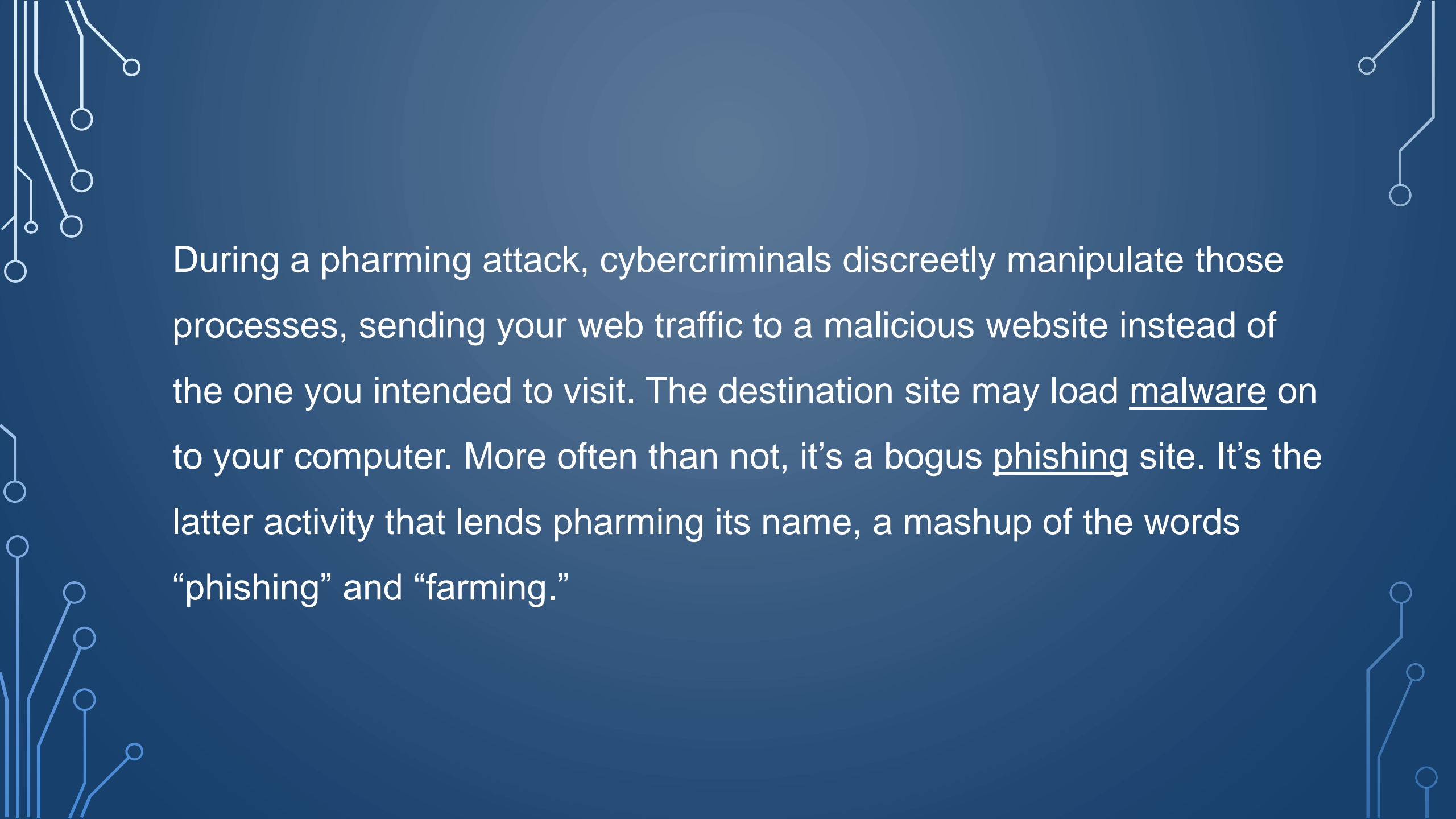
The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments connected by right-angle turns, ending in small circles, resembling a stylized PCB or network diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Vishing can be an extremely useful tool for attackers, because their targets do not have time to think the situation through prior to providing information to the attacker and can easily be confused by alarming claims.


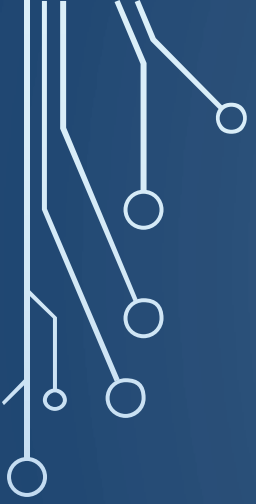
Pharming

Pharming is a type of cyberattack that involves redirection of web traffic from a legitimate site to a fake site for the purpose of stealing usernames, passwords, financial data, and other personal information.

When you type a URL into your browser's address bar, like www.google.com for example, several background processes have to happen before you see that familiar Google logo and search box on your computer screen.

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of vertical and horizontal segments connected by diagonal lines, ending in small circles, resembling a stylized network or data flow diagram.

During a pharming attack, cybercriminals discreetly manipulate those processes, sending your web traffic to a malicious website instead of the one you intended to visit. The destination site may load malware on to your computer. More often than not, it's a bogus phishing site. It's the latter activity that lends pharming its name, a mashup of the words “phishing” and “farming.”




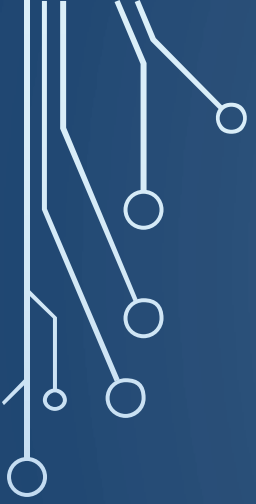
We have covered a lot of ways your computer can be attacked as well as what to be aware of and steps to take before clicking on a link, downloading an attachment, answering an email and myriad other attempts to obtain valuable information from you.





Here are a few review questions

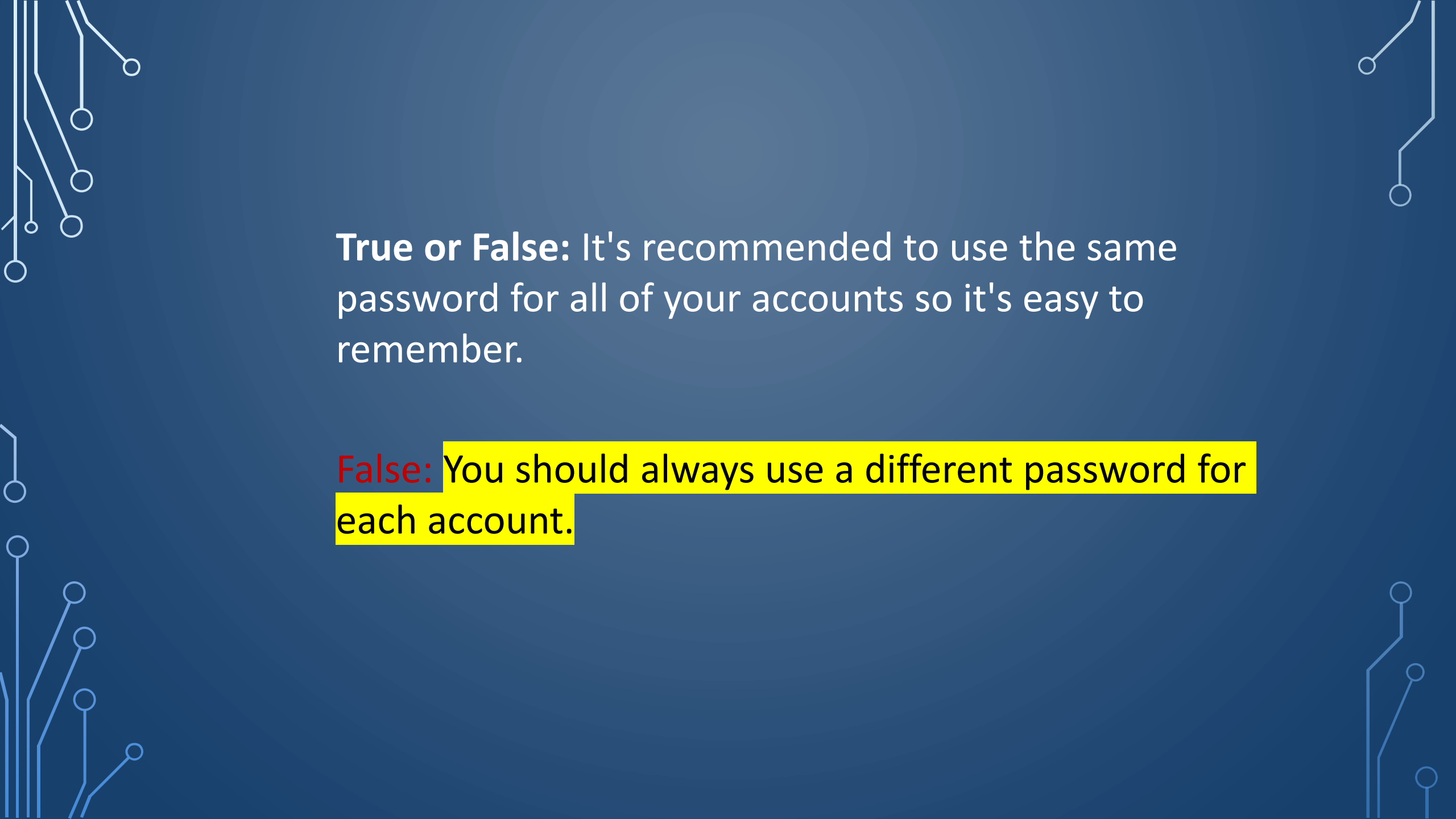
The background is a solid dark blue color. In the four corners, there are white line-art graphics that resemble circuit board traces or neural network connections. These lines are thin and end in small circles, creating a technical or digital aesthetic.

Review Questions



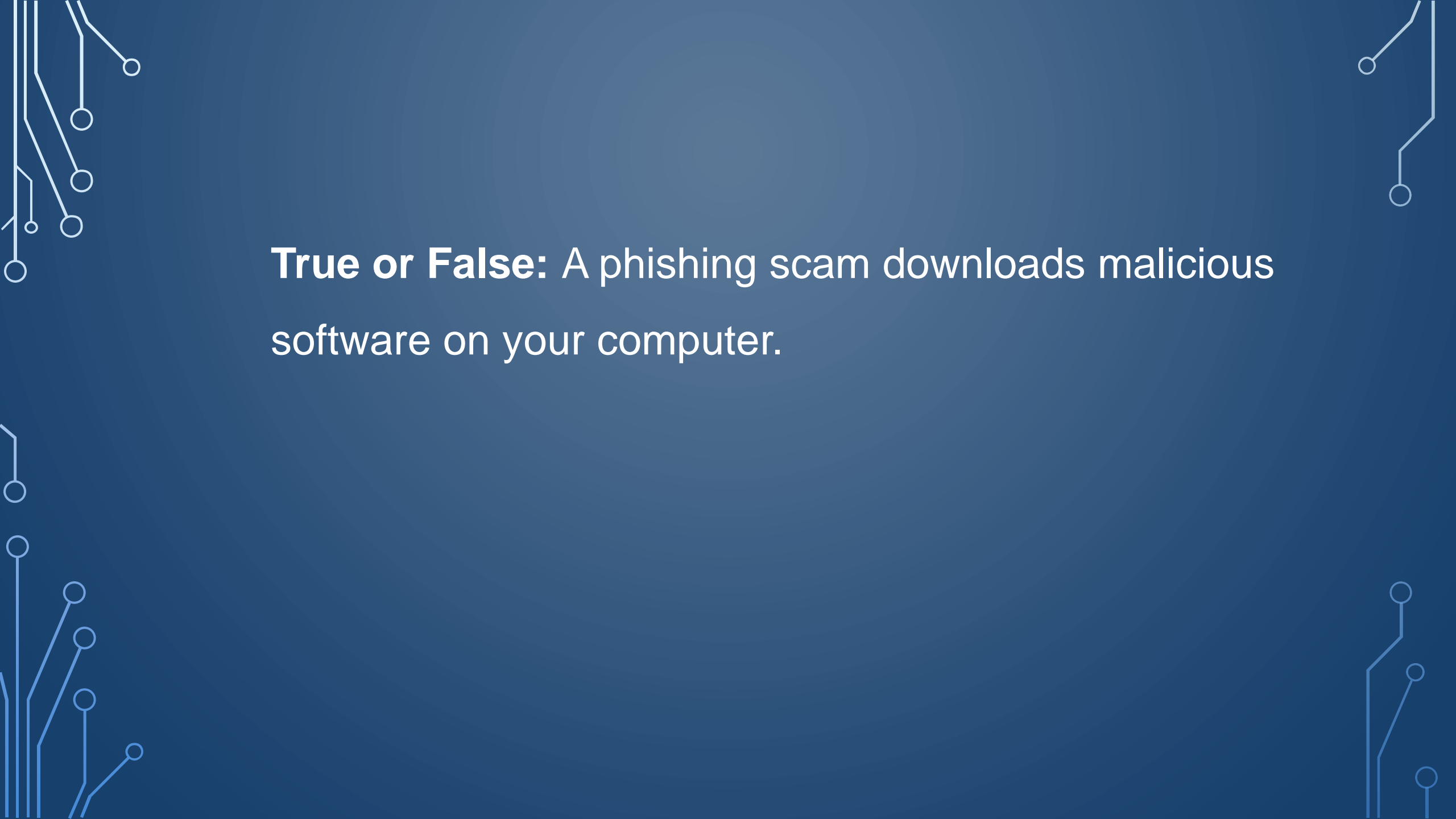
True or False: It's recommended to use the same password for all of your accounts so it's easy to remember.




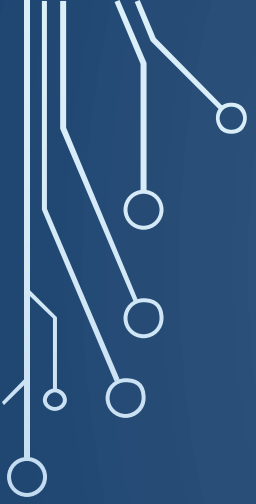
The background is a solid dark blue color. In the four corners, there are decorative white and light blue circuit-like patterns consisting of lines and small circles, resembling a network or data flow diagram.

True or False: It's recommended to use the same password for all of your accounts so it's easy to remember.

False: You should always use a different password for each account.



The background is a solid dark blue color. In the four corners, there are decorative white line-art elements that resemble circuit traces or network connections. These elements consist of straight lines of varying lengths and angles, ending in small white circles. The top-left and bottom-left corners have more complex, branching patterns, while the top-right and bottom-right corners have simpler, more linear patterns.

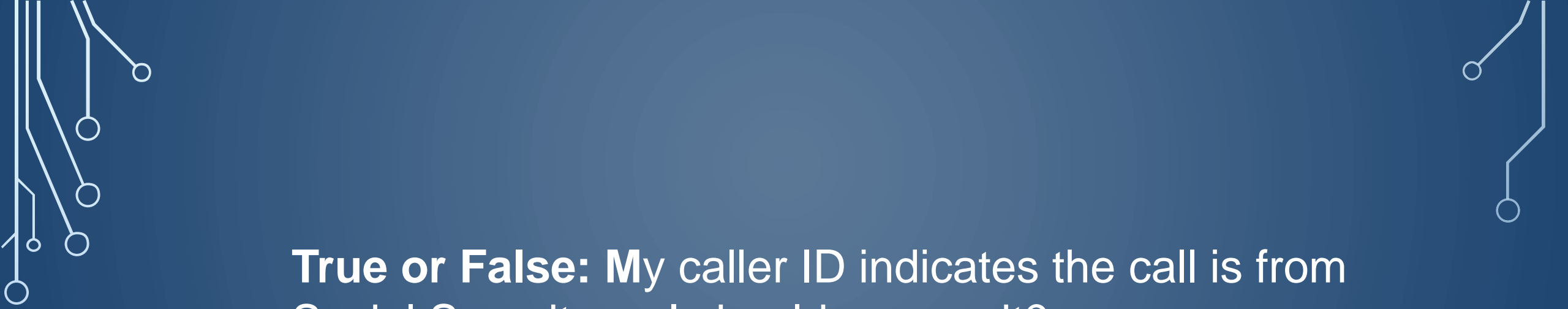
True or False: A phishing scam downloads malicious software on your computer.




True or False: A phishing scam downloads malicious software on your computer.

False: A phishing scam is designed to trick you into providing your confidential data to steal money or information.





True or False: My caller ID indicates the call is from Social Security so I should answer it?





True or False: My caller ID indicates the call is from Social Security so I should answer it?

False: This call is likely a *phishing* scam using a *spoofed* number. Social Security normally doesn't call!



Which of the following is something you should NOT do when backing up your data?

- A. Make sure your files are saved off-site
 - B. Routinely verify backups
 - C. Copy and paste all your files to the desktop
 - D. Use automated backup software
- 
- 

Which of the following is something you should NOT do when backing up your data?

- A. Make sure your files are saved off-site
- B. Routinely verify backups
- C. Copy and paste all your files to the desktop
- D. Use automated backup software

C: Copying and pasting your files to the desktop is not a means of backup.



That's all Folks!

The image features a dark blue background with white decorative circuit-like lines in the corners. These lines consist of straight segments and small circles, resembling a stylized PCB or network diagram. The lines are positioned in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

Thank you

Questions?