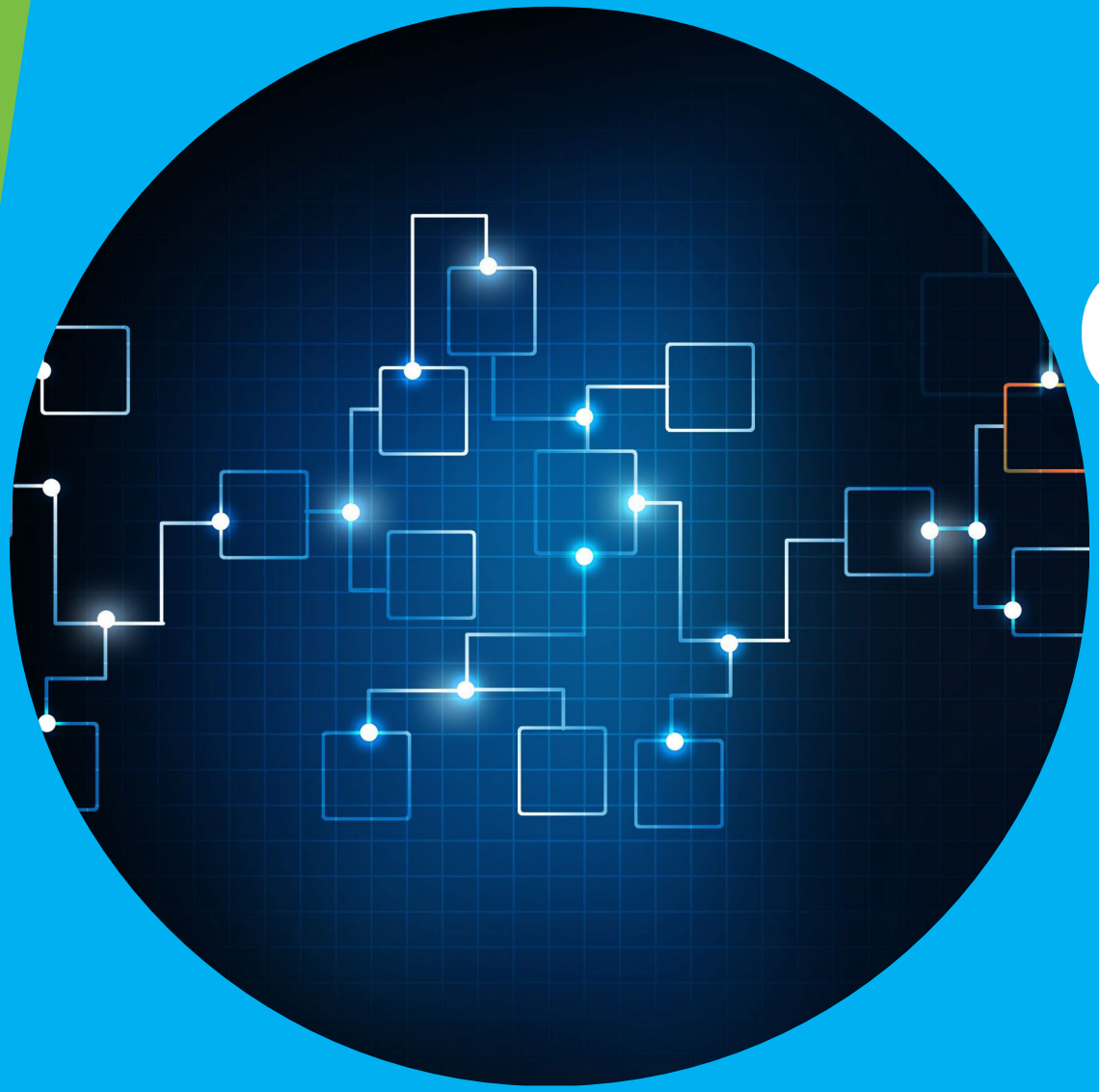


Cybersecurity & Fraud Training

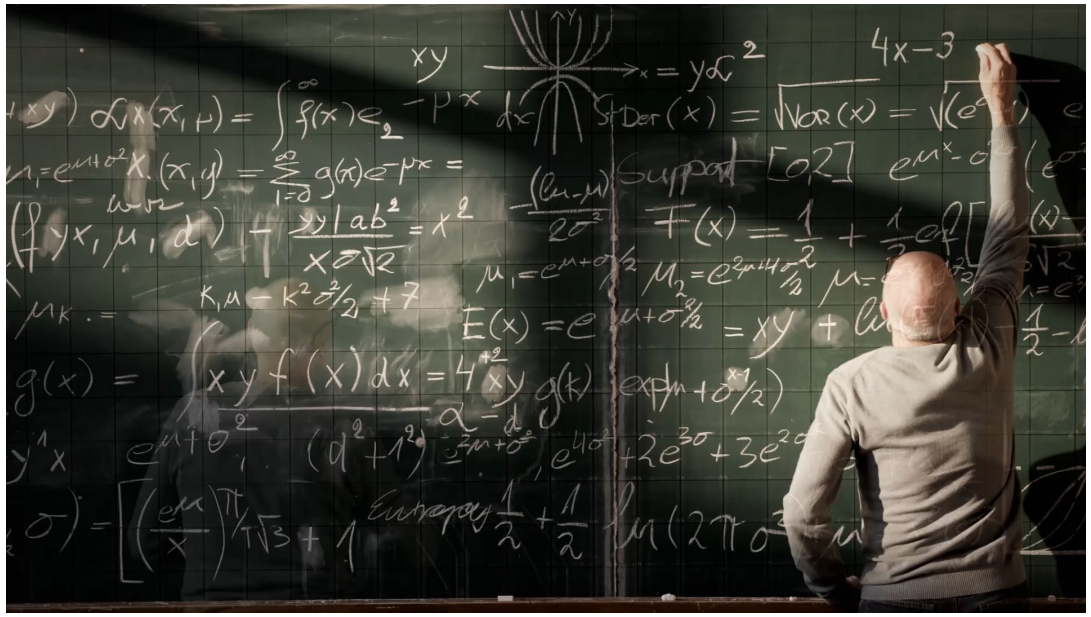
AAFCPAs
great minds | great hearts

Opener

- Do you have a fish tank in your home or office?
- If yes, please raise your hand in Zoom.

Learning Agenda

- What Threats Are Out There
- Social Engineering
- Email Security
- Phishing
- Mobile Devices
- Telework Security
- Physical Environment
- Internet of Things (IoT)



What Threats Are Out There

- **Viruses**
  - Target computers to cause disruption of service
- **Malware**
  - Malicious software that targets computers to cause disruption of service and/or attempts to steal personal information
- **Ransomware**
  - Malware that targets computers and encrypts all of the victim's data then demands payment to restore the access
- **Social Engineering**
  - A type of security attack where scammers trick people into giving them access to sensitive information
- **Phishing/Spear Phishing/Whaling**
  - Email techniques used to steal data or to lure you to send money
- **Full Hack Attack** that will take over you whole environment
  - Targets systems and people as means to steal personal and organizational sensitive information that can be used against you or the organization

Social Engineering

- Focus on tricking people rather than breaking into networks
- Social Engineers are very patient!
- Create a sense of urgency
- Use of Artificial Intelligence
- Attack Methods:
  - Online and Phone
    - phishing emails and smishing (SMS/text messaging)
    - social networks
      - research personal details and use this information to hack into accounts
      - create fake social media profiles and pages containing embedded malware, strange links in social media posts, apps requesting you to enter your profile information

Social Engineering

- Attack Methods:
  - Human Interaction
    - Phony vendor visits (HVAC, printer repair, pest exterminator)
    - Random person bringing treats to the office
    - Pretend to have left something behind from a previous visit
    - Piggy-backing into a secure building
    - Gain trust by using humor
  - Passive Tactics
    - Dumpster diving for tossed out invoices, confidential documents, printed emails, discarded computers and mobile devices
    - “Shoulder surfing” which can be done in person or remotely with cameras /software

Email Security
Basics to keep in mind

- Email is NOT encrypted.
- Email can accidentally be sent to the wrong email address.
- Once an email message has been sent, you no longer have control over the message. It can be forwarded to anyone by the recipient.
- Never send login credentials through unencrypted email.
- Never send confidential information through unencrypted email.
- Be wary of links and attachments in unsolicited email messages.

Phishing
Red Flags to look for

- Inspect the email content
  - Tone
  - Grammar, punctuation, spelling
  - Attachments or links
  - Logos
  - Sense of urgency
  - Asking for personal information

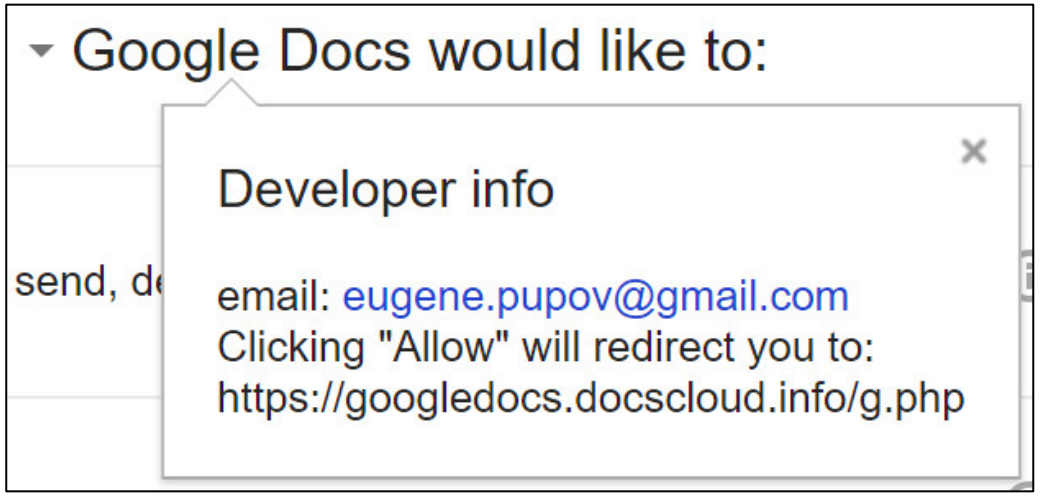
- If there are links in the body of the email hover the pointer over them and look at the bottom right corner of your screen or the pop up for the full address
- Is it addressed to you or is it generic (even though hackers are becoming more and more personal)
- If it's too good to be true it's most likely a scam

Phishing
Hyperlinks – Inspect for link manipulation

- http vs https
- Hover over link to verify website redirection
- Scrutinize the link
  - https://www.bankofamerica.com/login
  - https://www.bankofammerica.com/login
  - https://wwwbankofamerica.login.com
  - https://143.127.22.13/bankofamerica.com/login
- Tiny URL – http://goo.gl/3akWbr

Phishing

Example 1 – Google Docs Phishing Attack



- Emailed invitation from someone you may know
- Real google login screen
- Asks you to continue to Google Docs
- OOOOOOOPPPPPPSSSSSS you just gave access to your email and address book to a cyber criminal
- Check the title for developer information…

Phishing
Example 2

Phishing
Example 3

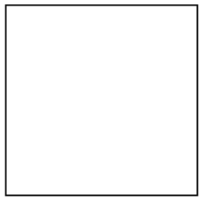
From: achremittance@tregolls.cornwall.sch.uk via SurveyMonkey <member@surveymonkeyuser.com>
Sent: Friday, August 14, 2020 10:07 AM
To: [redacted]
Subject: *EXTERNAL*- inv# 55356, 73667 and 82673 has been processed

[redacted]

inv# 55356, 73667 and 82673 has been processed and paid today.

VIEW INVOICES AND REMITTANCE COPY

Please do not forward this email as its survey link is unique to you.
Privacy | Unsubscribe



Phishing
Example 4

Attached  Voice Message.pdf
51 KB

-----Original Message-----
From: Support <jsmith@xyzco.com>
Sent: Thursday, August 6, 2020 2:13 AM
To: Jeff Smith <jsmith@xyzco.com>
Subject: You have a new voice message

A message was recently left in your voice mail account.

We are sending you this email because you have asked for your messages to be forwarded to this address.

The original message is still in your account, and will be played or shown as usual the next time you log in. If you prefer, you can use the link below to delete it. You can also mark messages as "heard", which means they will be kept in your voice mail account, but will not be treated as new messages.

Phishing
Example 5

From: DHL team <noreply@yourdhl.maintenance.com>
Sent: Saturday, August 22, 2020 7:16 PM
To: [redacted]
Subject: *EXTERNAL*- Parcel arrival Notice

Dear shipper,

Your parcelle has arrived at post office on Tuesday August 18 2020

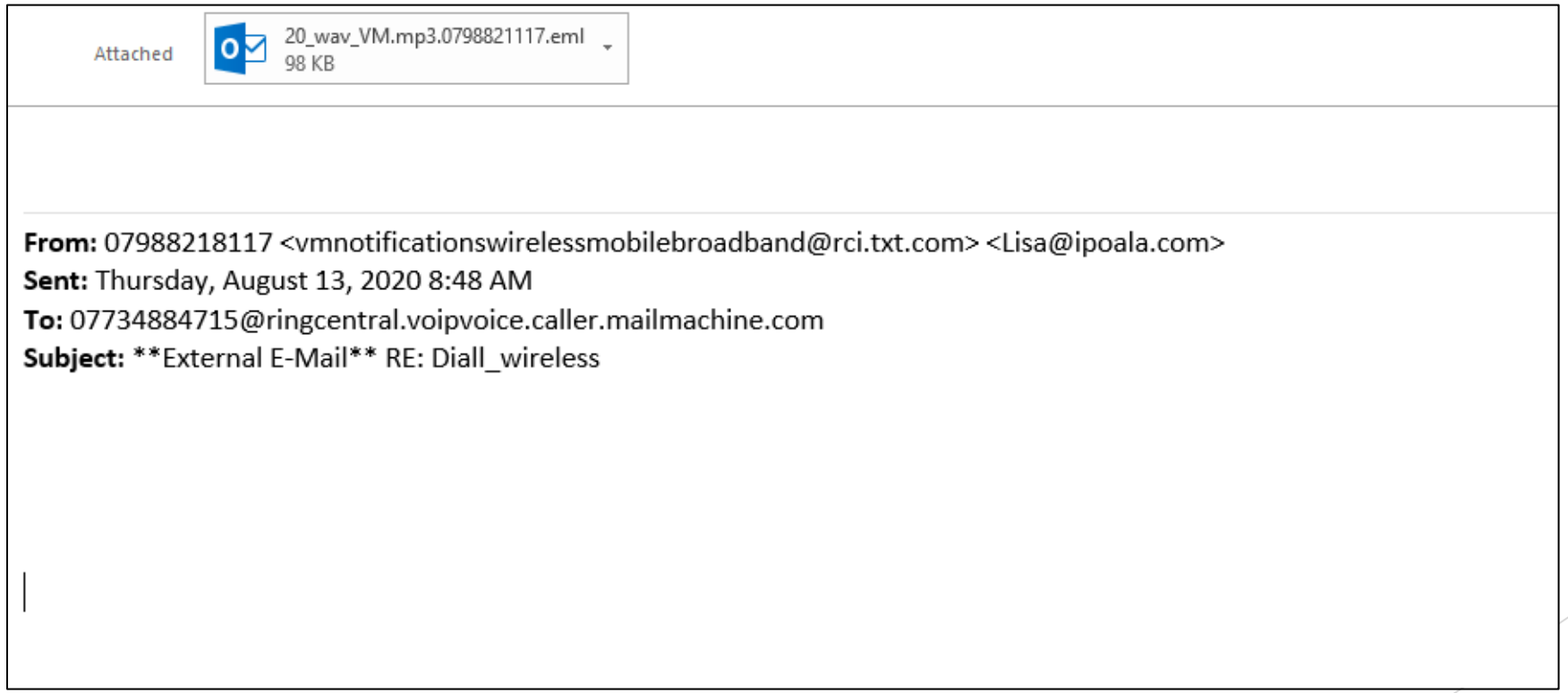
Tracking No: 51287594476463

Please kindly fil out tracking number by clicking on the DHL Tracking link to claime your parcel or it will be returned to original destination!

Thank you for your support.

Regards,

Phishing
Example 6



Phishing
Example 7

From: CallCenter <jillt@scolaromasonry.com>
Sent: Tuesday, July 21, 2020 1:06 PM
To: [redacted]
Subject: *EXTERNAL*- You've a new call recording [Action Reuqired]
Importance: High

Hello ,

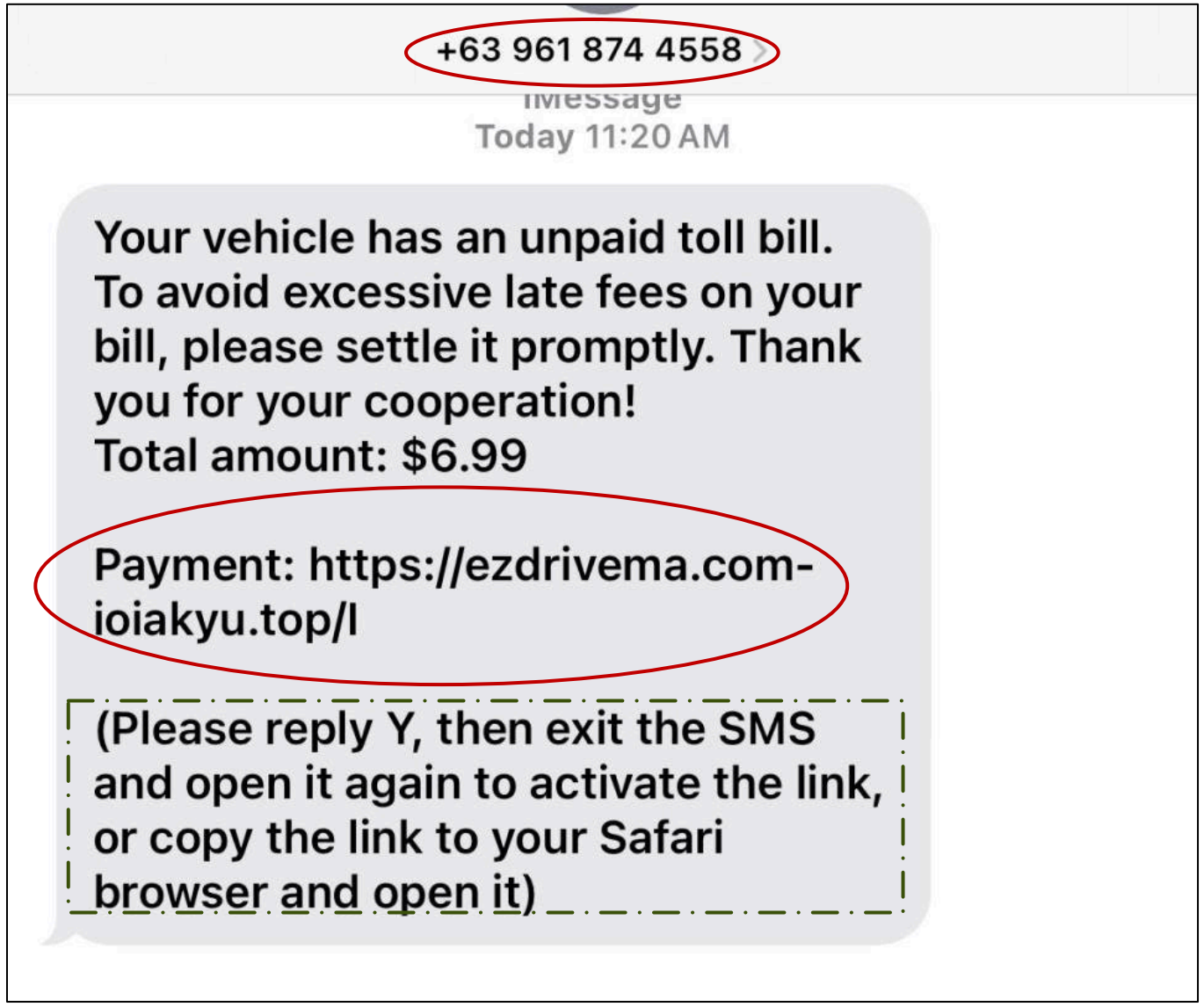
Your Virtual Office Extension has a new voicemail.

New voicemail details:

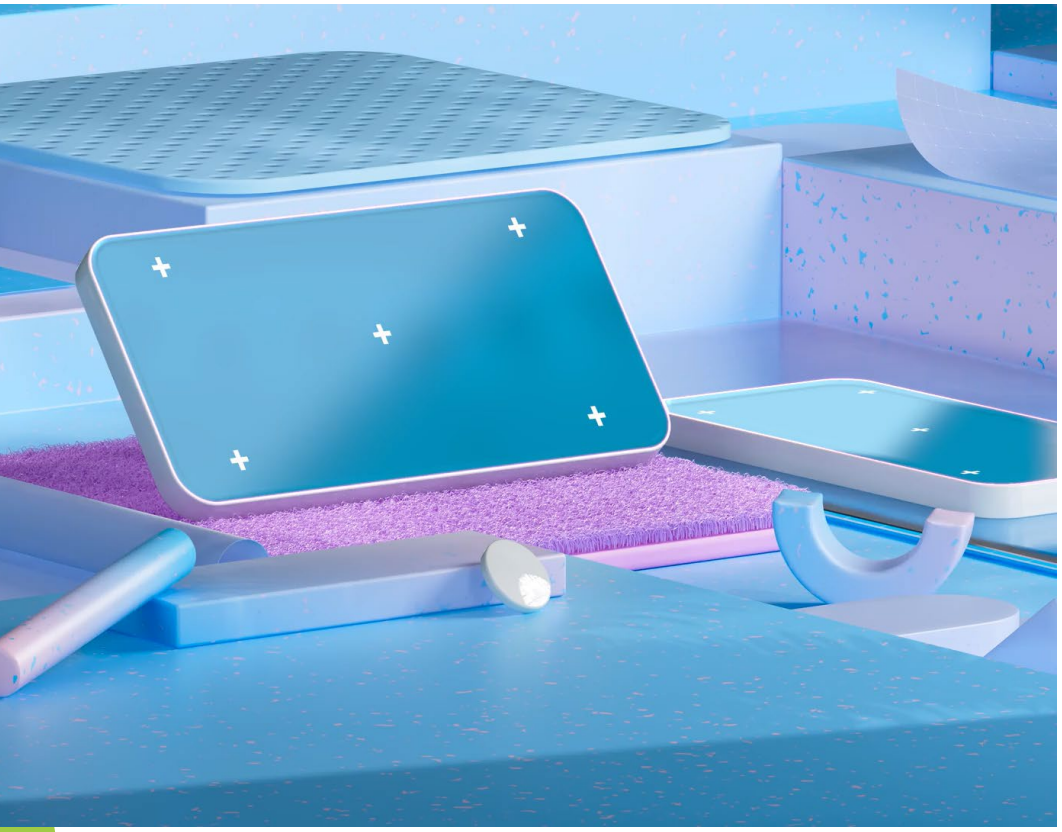
Received from:	1-716-902-2389 WIRELESS CALLER
Date/Time:	21 July, 2020 10:06
Duration:	20 Seconds
Listen/Download:	PLAY - VM - 05-11-2020 - 780302789 .wav

- Please note that you can download to listen to the Vmail that was sent to
- No third-party access.

Smishing


+63 961 874 4558
Message
Today 11:20 AM
Your vehicle has an unpaid toll bill. To avoid excessive late fees on your bill, please settle it promptly. Thank you for your cooperation!
Total amount: $6.99
Payment: https://ezdrivema.com-ioiakyu.top/l
(Please reply Y, then exit the SMS and open it again to activate the link, or copy the link to your Safari browser and open it)

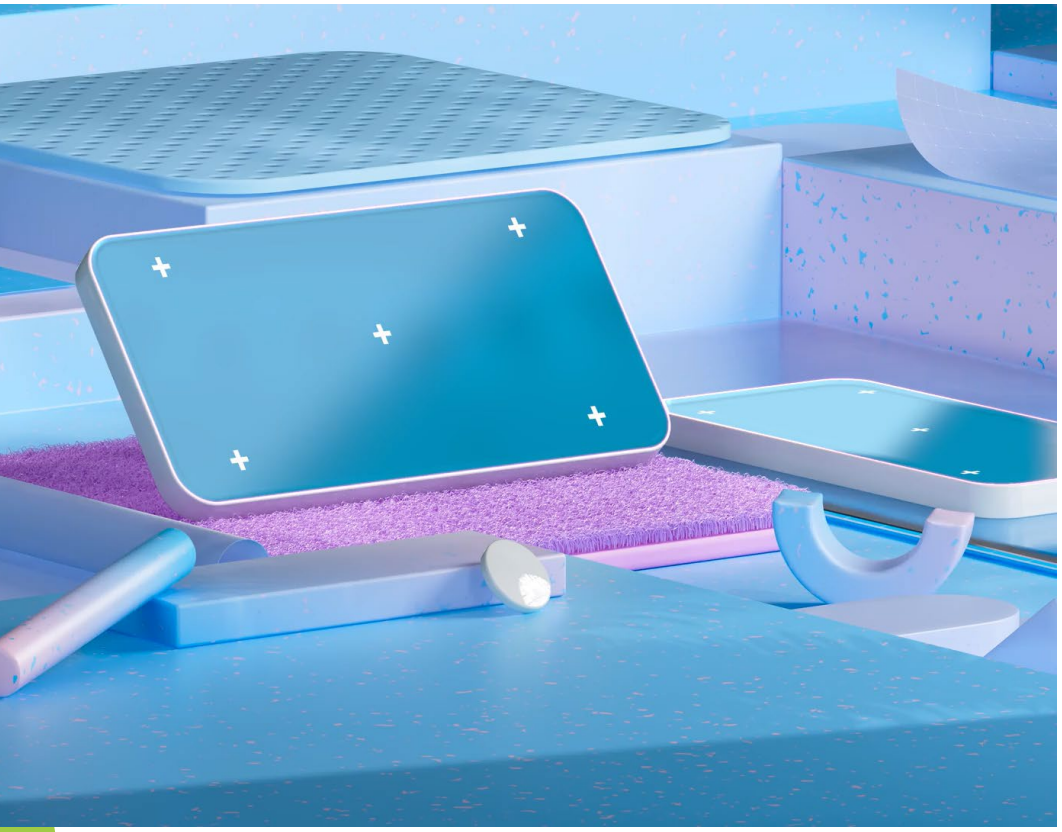
Mobile Devices



- Mobile devices include tablets, smartphones, wearable devices (e.g. smart watches), laptops/notebooks, and USB devices

- There are benefits to these devices, but they also introduce risks to a business and individuals

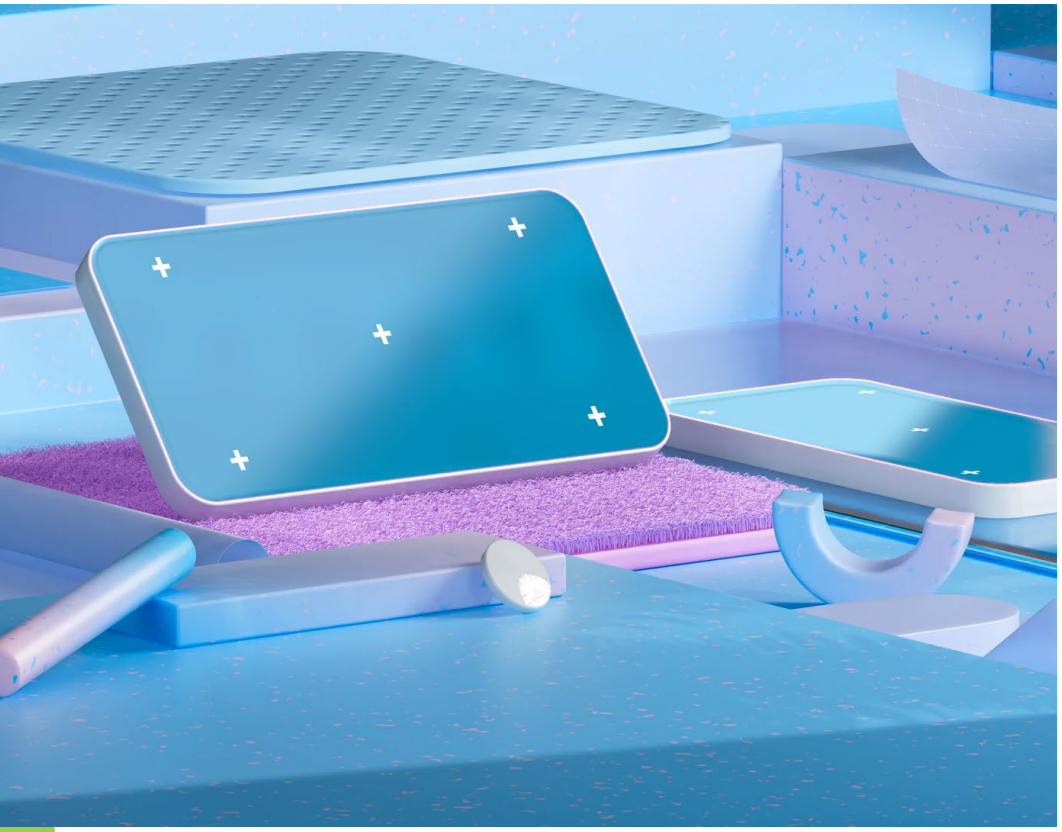
Mobile Devices



Think about all the different questions that come to mind if a mobile device is stolen:

- Will I get my device back?
- Who do I contact for help (work, cell carrier)?
- Is the data on my mobile device backed up (photos, videos, personal data)?
- Are my email, bank, social media accounts at risk?
- Is my organization's data at risk?
- Can my device be remotely wiped?

Mobile Devices
Physical Safeguards



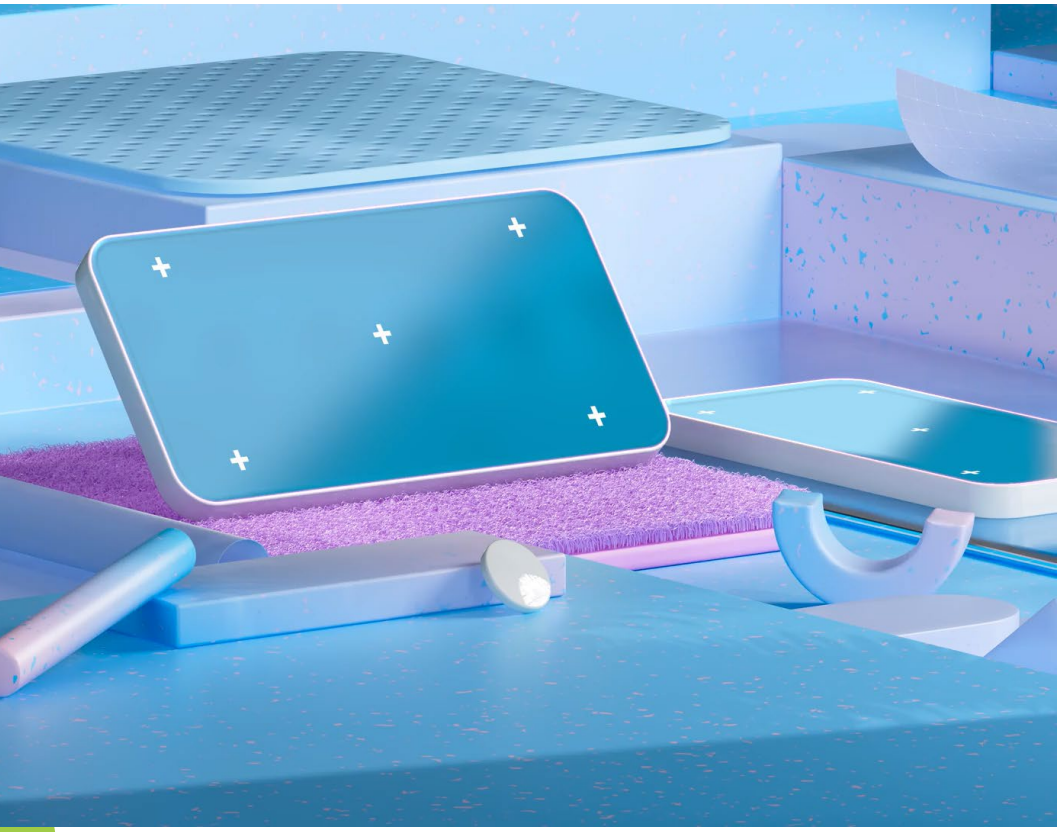
It's always good to plan ahead and take precautions with your mobile device.

Keep the device in a secure location when not using it, either:

- In a closed bag
- On your person

Stay alert in crowded places as you can be easily distracted.

Mobile Devices
Technical Safeguards



- Lock your device when not in use
  - Biometrics, PIN, passphrase/word, swipe code. Use the strongest locking mechanism available.
  - Laptops at home for telework
- Encrypt your data – puts your data into an unreadable form
- Regularly back up your data so it can be easily restored
- Implement a solution to remotely wipe/delete your data
- Enable GPS, e.g. Find my Phone (check your organization's policies first)
- Know who to contact if device is stolen

Telework Security

Safety considerations when working remotely (teleworking)

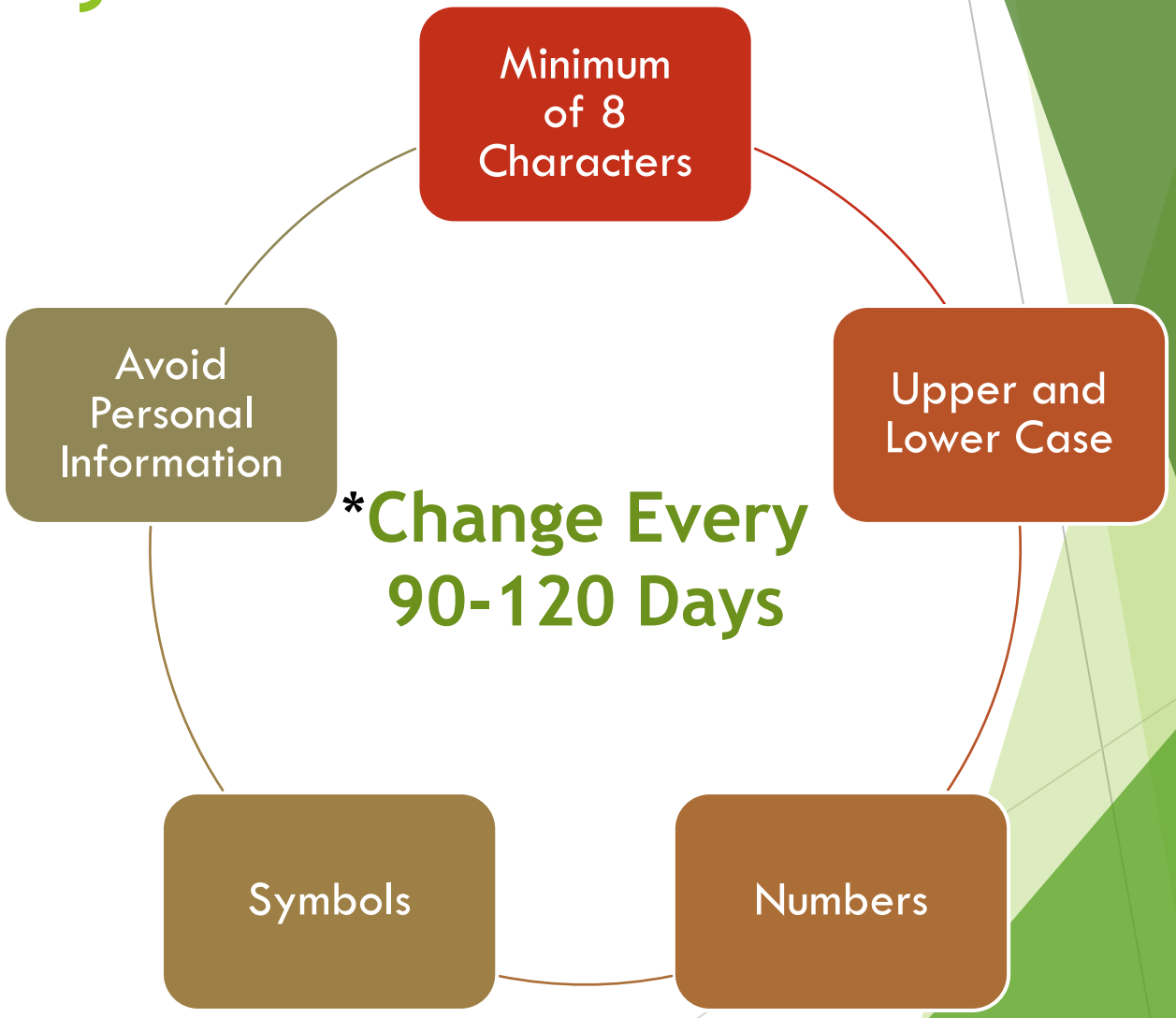
- Passwords / Multi-factor authentication
- Secure connection to the organization's network (remote access options)
- Creating a secure "Home Office" for teleworking

Telework Security
Passwords

- A complex password should be hard for others to guess and easy for you to remember. This is the first line of defense in protecting both personal and the organization's data.

Telework Security
Passwords

- A complex password should be hard for others to guess and easy for you to remember. This is the first line of defense in protecting both personal and the organization's data.



Telework Security
Multi-Factor Authentication (MFA)

- We know data breaches and phishing attacks expose passwords, so multi-factor authentication should be used for additional security to our online accounts including our work accounts.

- MFA is a security measure that requires at least two independent factors to be able to log into an account. It's what you know and what you have.

- Examples:
  - House key and alarm system
  - Bank ATM card and PIN #

Telework Security
Multi-Factor Authentication (MFA)

- Priority accounts that should have MFA
  - Email (we have a lot of information in our email that hackers would like to have!)
  - Social media accounts (personal and work-related)
  - Financial accounts
  - Password managers

- Other items to secure
  - cell phones, key fobs, USB devices

Telework Security

Remote access connection to the network

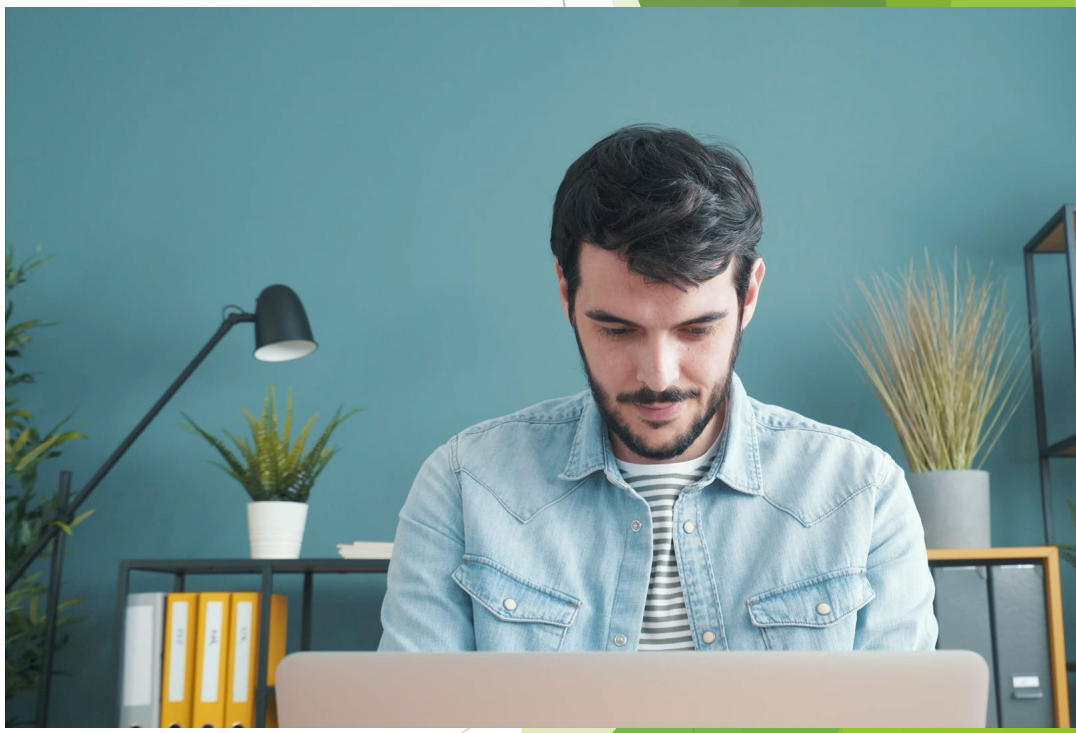
- Your organization's confidential information should either be accessed via a secure remote connection to the company servers or left at the office.

- Connection to your organization's network needs to be secure
  - Virtual Private Network (VPN)
  - Virtual Desktop Interface (VDI)

Telework Security

Safety Measures for Your "Home Office"

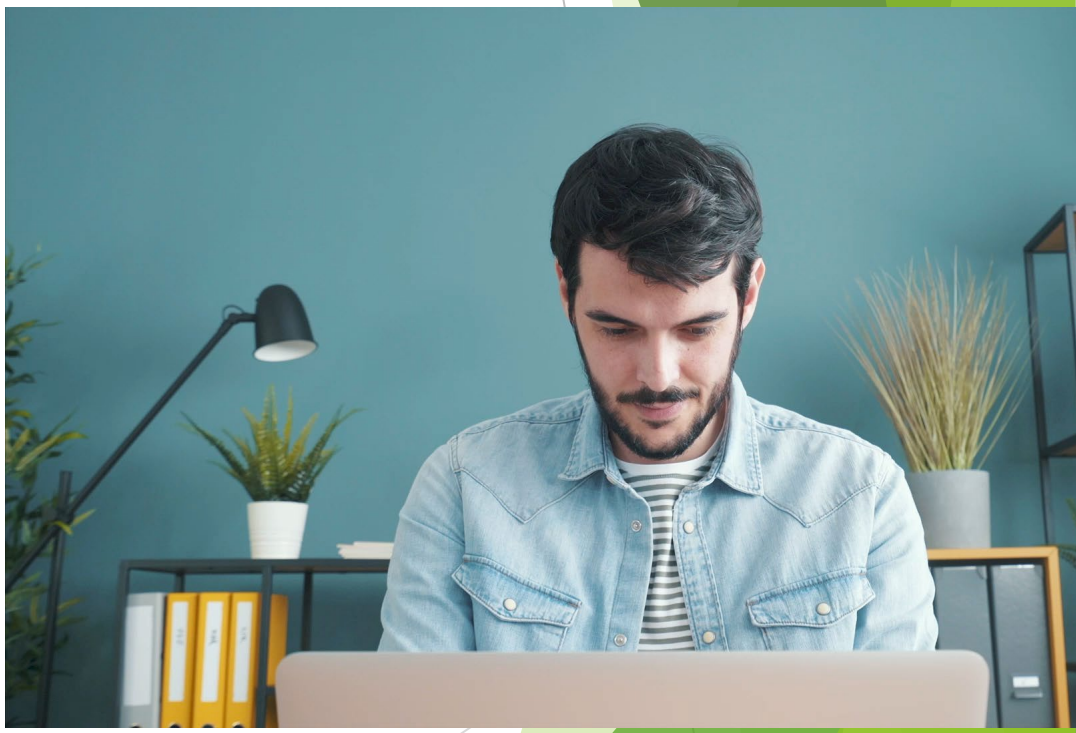
- While working in your home office avoid using corporate devices for personal use.
  - Don't let friends or family members use corporate devices
  - You are responsible for the security of this device and any data that may be save on it
- Unless authorized by your organization, the general rule is to not use personal devices to access corporate systems or work on corporate projects.
- Do not share corporate credentials with family members.



Telework Security

Safety Measures for Your "Home Office"

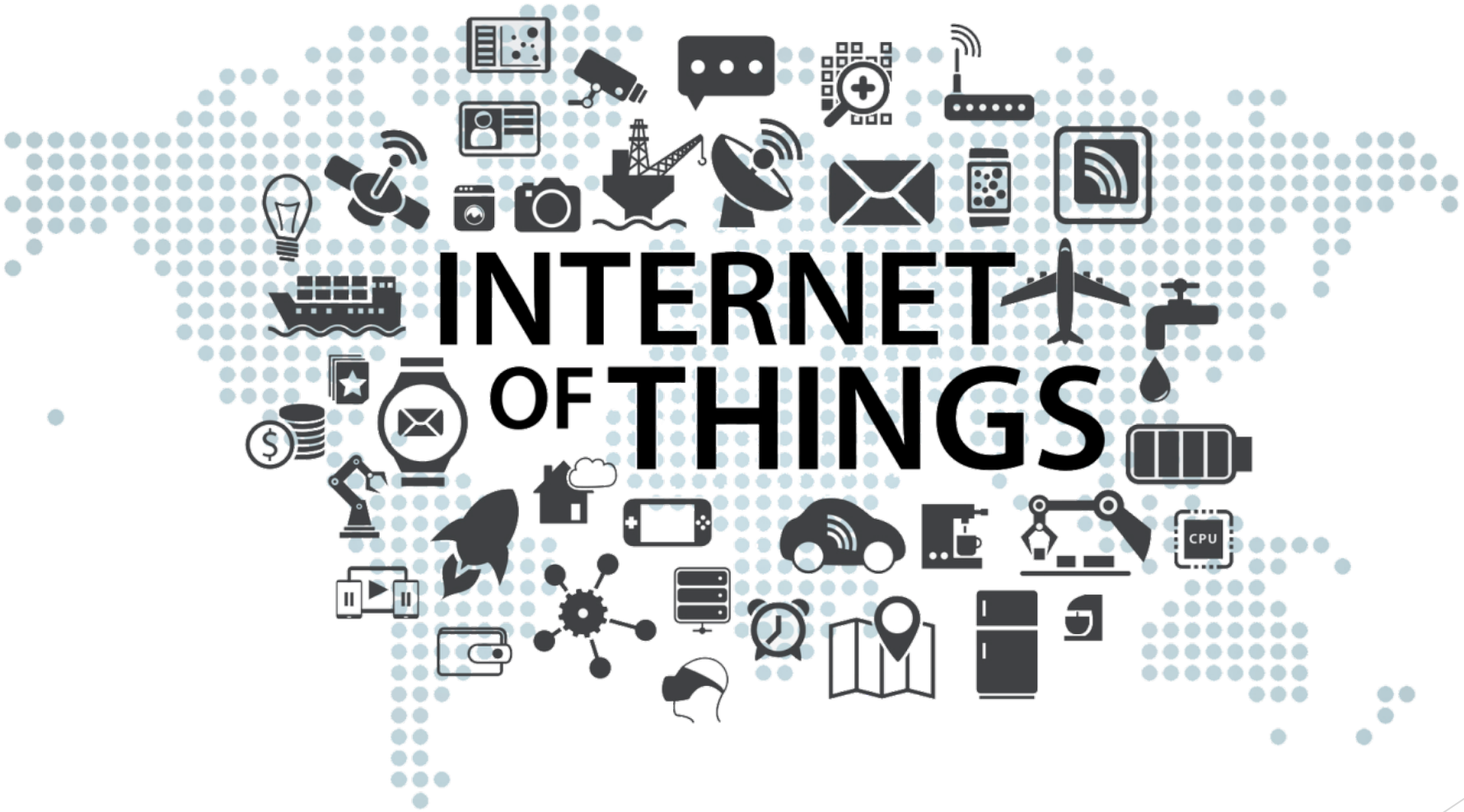
- Ensure your computer equipment is secure in the telework environment
  - Safe place to secure laptops when you're not home.
  - Is the computer hard drive encrypted?
  - Patching
- Securely dispose of any printed corporate information
  - remember compliance privacy
  - Organization's Privacy Policies
- Do not install unapproved software or unauthorized apps on corporate devices
- Do not turn on file sharing to sync data back and forth from your personal laptop and a work laptop when working from home.
- Follow your organization's backup policies and procedures to protect the integrity of the organization's data
- Do not store your organization's data on your personal file sharing site.



Telework Security
Securing Home Wi-Fi

It's important to have a secure internet connection while teleworking. Just as you shouldn't connect to free public WI-FI, you should also take steps to secure your home internet connection.

- Create different VLAN (virtual local area network)
- Highest level of encryption
- Change the default password for your wireless network
- Change the default admin password for your router
- Disable the "guest" network when not in use (if your router has this feature)
- Don't name your network with your name, address or other personal information
- Hide your network from broadcasting
- Xfinity customers: disable the Xfinity hotspot feature


INTERNET
OF THINGS
CPU

Internet of Things (IoT) *Overview*

- An increasing number of companies are installing IoT devices on their networks. IoT devices are typically “black box” devices, the inner workings of which are unknown to most users.
- For example, HVAC systems, smart fridges, computer printers, and even cars can contain IoT-enabled technology that connects through WiFi or cellular and therefore can be considered IoT devices.

Internet of Things (IoT)
What Is It?

Examples (Home)

- Car- service scheduling and monitoring
- Fitbit- health tracking
- Refrigerator or dishwasher- performance issue or tells you to buy milk.
- Thermostat- controls heating and cooling based on occupancy.
- Baby monitor- check in on junior.
- Hot water heater- vary temp or vacation mode

Examples (Office)

- The vending machine in your office
- Internet based wireless phones
- Printers
- Alarm systems
- HVAC systems
- Lighting automation
- Electric and gas metering
- Health monitors- for insurance premium reduction

Internet of Things (IoT)
Does this look familiar?

Things
Cell Phone
Thermostat

Gateway
Home/Work Router

Network
(oh Boy)

Applications
Financial Applications
Personal Data

Microsoft Dynamics GP

Internet of Things (IoT)
Security Concerns

How Complex are the admin/user passwords?

Default Accounts (Admin and Manufacturer)

Is it a blessing or curse?

Internet of Things (IoT)
Security Concerns

What standards are used?
*Are they secure? Is your **fish tank** secure?*

Software for some of those devices is low quality.

Where is the data going and who has access to it?

Internet of Things (IoT)
What can you do?

- Assess! Assess! Assess!
- Be Up to Date with Patching
- The Most Current & Secure Ways to Communicate
- Segregate IoT Devices from Other Systems
- Perform Vulnerability & Penetration Tests – Phishing
- Educate / Inform

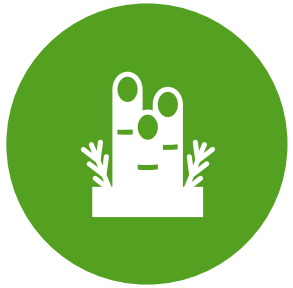
Physical Security
Overview

- Data and IT Security goes well beyond cyberspace. The security of your physical office space may also be at risk.
- A successful physical breach by an outsider could produce unauthorized access to packages, equipment, documents, as well as threats of theft and employee safety.

Physical Security
Examples of Potential Threats

- **Driveways / Street Parking / Parking Lots**
  - USB flash drive
  - Laptop stolen from car
  - Burglars & physical injuries
- **Piggybacking**
  - Piggybacking, or the close following of an employee through company entrances, is a risk to physical office spaces during business hours.
  - Once intruders gain discrete access to your office, they could steal equipment or install devices on your network, which would then allow them to access your systems remotely.

Physical Security *Recommendations*



Unobstructed Views -

AAFCPAs advises clients to evaluate risks posed by view obstructions, such as overgrown shrubs or poor exterior lighting.

Locked Workstations -

Employees should be expected and reminded to lock their computers /workstations when they leave their desks.

Clean Desk Policy -

Employees should remain vigilant about what is accessible/visible on their desk, such as client information, account passwords, or other sensitive data.

See Something, Say Something -

Employees should be encouraged to greet all unfamiliar faces and offer assistance, as well as ask why they are there. As an additional precaution, AAFCPAs suggests that management implement photo IDs for employees and badges for all visitors

Closer
Reflecting on Cyber Fraud Training

- Do you feel you can effectively keep your information systems and personal information safe?
- Do you think you can effectively mitigate cyber security risks using the methods presented?

AAFCPAs
great minds | great hearts

Thank You

AAFCPAs
great minds | great hearts