THE OFFICE OF THE BISHOP PRESENTS

CYBERSECURITY

A Webinar from the Diocese of Olympia

The Episcopal Church in Western Washington

What is Cybersecurity?

Cyber Security: *"The protection of an organization and its assets from electronic attack, to minimize the risk of business disruption"* --- IBM

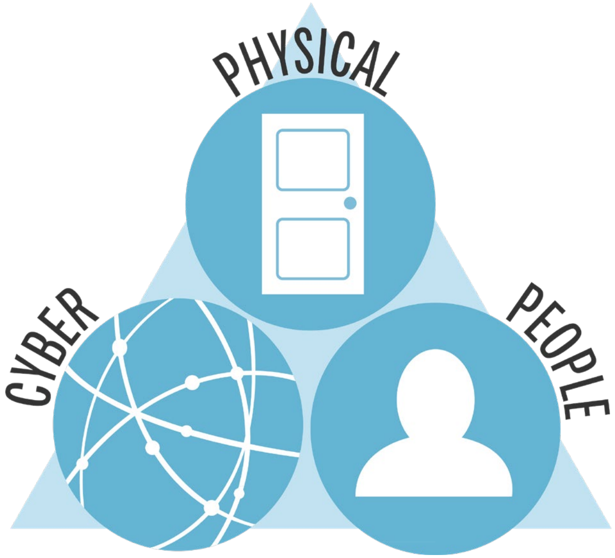
Not just the organization, but also you in your daily life

Agenda

- Threats Overview
- Password Safety
- Internet Protection
- Email Protection
- Preventive Measures

3 Components of Cybersecurity

Doors, locks, security cameras



IT Staff - Ex. firewalls

(Most Vulnerable)

- Remember to lock the lock
- Remember to close the door
- Don’t allow others to tailgate
- Make door is not propped open
- Keep tight control of the key

Malware

- There are numerous variations
  - Viruses
  - Worms
  - Trojans
  - Ransomware
  - Rootkits
  - Bootkits

Malware

- On average, 390,000 unique threats per day.
- Unique threats ≠ extremely dissimilar.
- Malicious threats are changed in the smallest amount possible to evade detection.
- Malicious threats are targeted in order to have the highest penetration (success) rate.

Malware

- Malware exists on other operating systems (OSes) outside of Windows.
- Windows is typically the major target due to high market share.
- When new malware is released on other OSes, it typically has a high penetration rate due to people believing their Android, Mac, and Linux devices are safe without having any endpoint security installed.

Malware

- Mobile phone malware is a growing threat due to users doing the majority of their internet browsing on a cell phone.
- Ransomware, or screen locking malware, is a popular threat on mobile devices.
- In 2016, malware targeting Apple iOS (iPhones, iPads) increased. Apple doesn't allow vendors to create antivirus for these products, so users must depend on the company to fix any vulnerabilities

How do you get infected

- Clicking malicious links in email
- Plugging in an unknown flash drive
- Downloading malware masquerading as other software
- Installing 3rd party apps directly from the internet instead of via official stores such as Google Play or Apple’s App Store.

How to Avoid Malware

- Install Endpoint Security on all devices
- Be careful what you plug in
- Be careful what you click
- Get awareness training for entire family.

Phishing

- Intentionally deceiving someone by posing as a legitimate company.
- Typically, utilizes email by pretending to be a company or service requesting you to do something.
- Hoping that you click the link and fill out the requested info

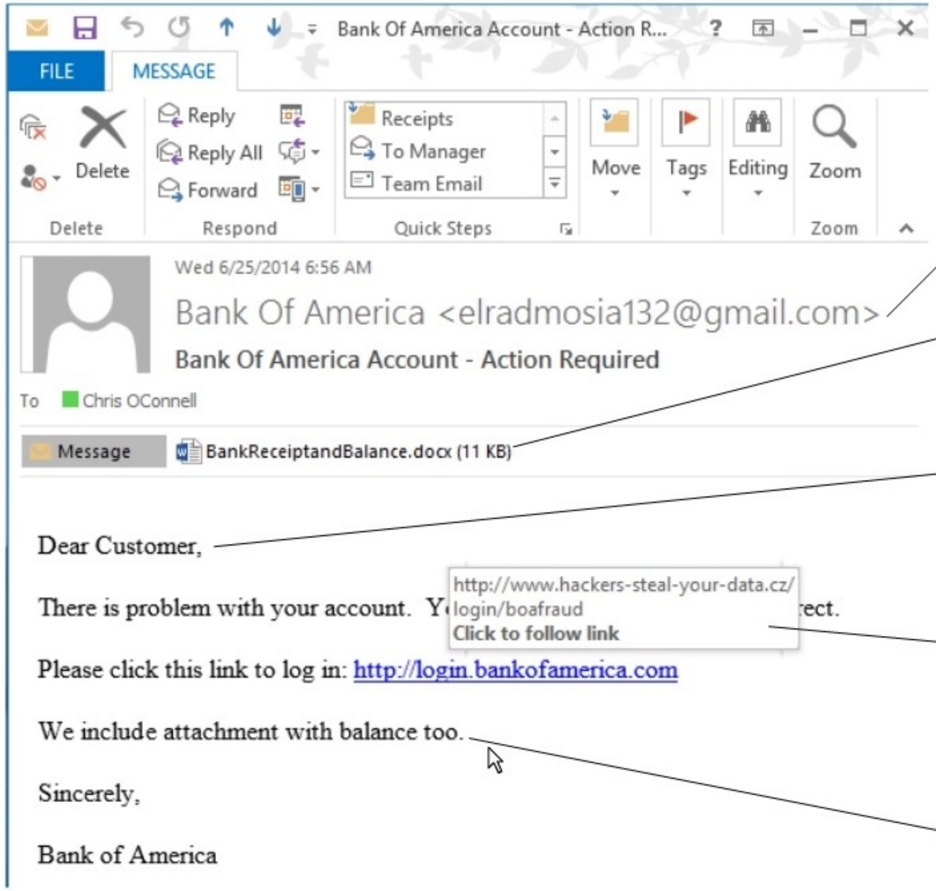
Phishing Terms

- Spear phishing – targeting selected individuals
- Whaling - the targets are high-ranking bankers, executives or others in powerful positions or job titles.
- Ransomware – holding your data hostage, phishing is primary way it spreads
- Website forgery and Covert Redirect – hijacking URLs

Email Security - Phishing

- A form of social engineering
- Malicious individual tries to trick you into giving up information or taking an action using:
  - Urgency
  - Fear
  - Authority
  - Information request
  - Something for nothing
  - Your mission

Examples of a Phishing Email



Wed 6/25/2014 6:56 AM

Bank Of America <elradmosia132@gmail.com>

Bank Of America Account - Action Required

To Chris OConnell

Message | BankReceiptandBalance.docx (11 KB)

Dear Customer,

There is problem with your account. Y[tooltip]ect.

http://www.hackers-steal-your-data.cz/login/boafraud
Click to follow link

Please click this link to log in: http://login.bankofamerica.com

We include attachment with balance too.

Sincerely,

Bank of America

Email says it's coming from a company, but is actually from a personal email service.

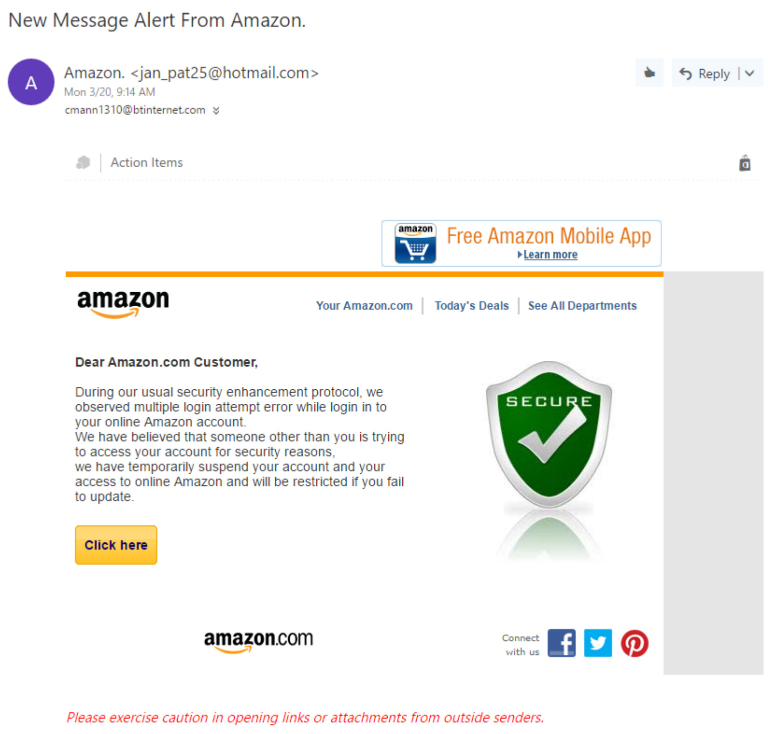
Never open attachments unless you're 100% sure they are from a trusted source.

Be wary of generically addressed emails!

Hover over a link without clicking. This shows where the link will actually take you. **If you don't recognize the site don't click!**

Grammatical or spelling errors indicate a fake!

Examples of a Phishing Email



New Message Alert From Amazon.

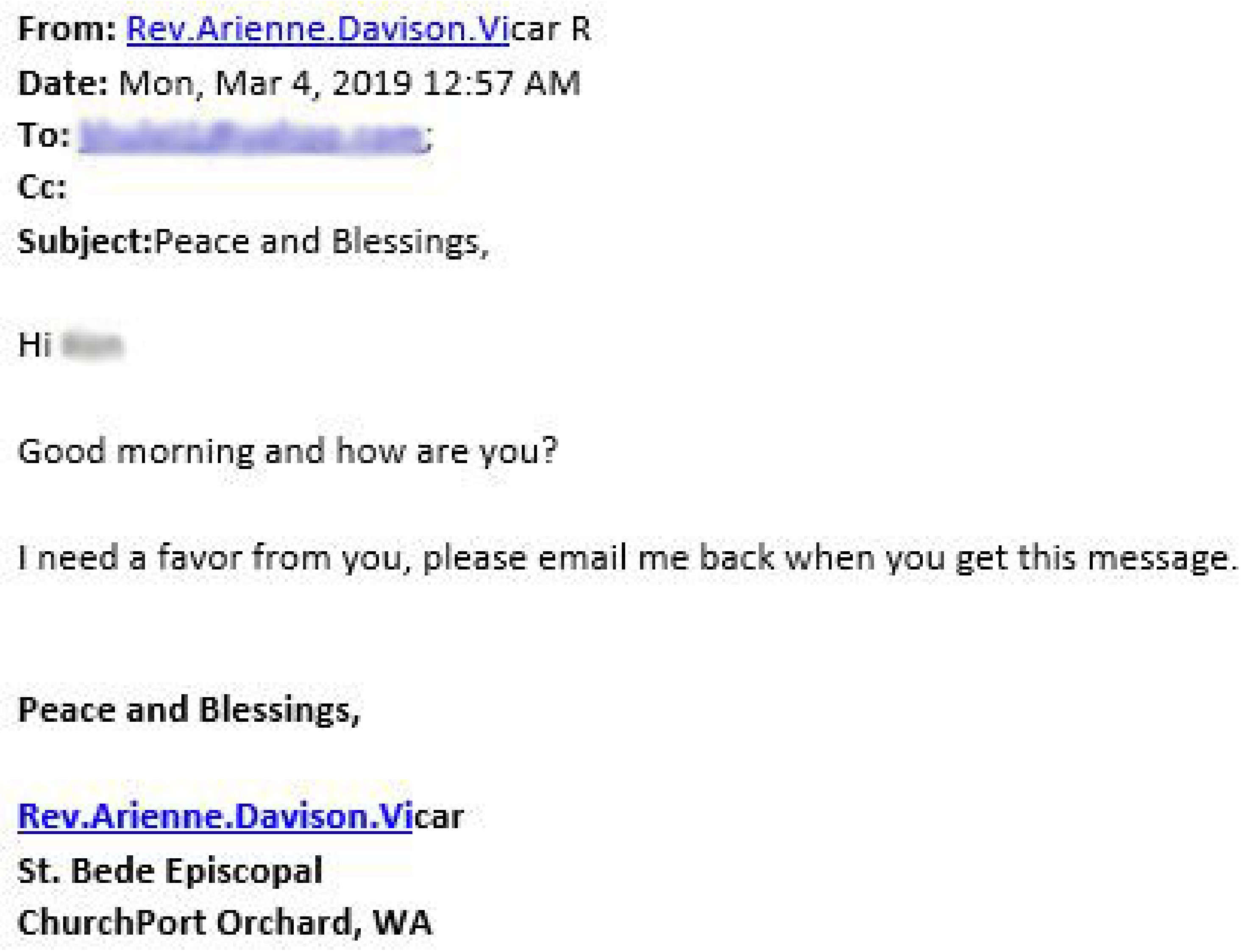
Amazon. <jan_pat25@hotmail.com>
Mon 3/20, 9:14 AM
cmann1310@btinternet.com

Dear Amazon.com Customer,

During our usual security enhancement protocol, we observed multiple login attempt error while login in to your online Amazon account.
We have believed that someone other than you is trying to access your account for security reasons,
we have temporarily suspend your account and your access to online Amazon and will be restricted if you fail to update.

Click here

Please exercise caution in opening links or attachments from outside senders.



From: Rev.Arienne.Davison.Vicar R
Date: Mon, Mar 4, 2019 12:57 AM
To: [redacted];
Cc:
Subject: Peace and Blessings,

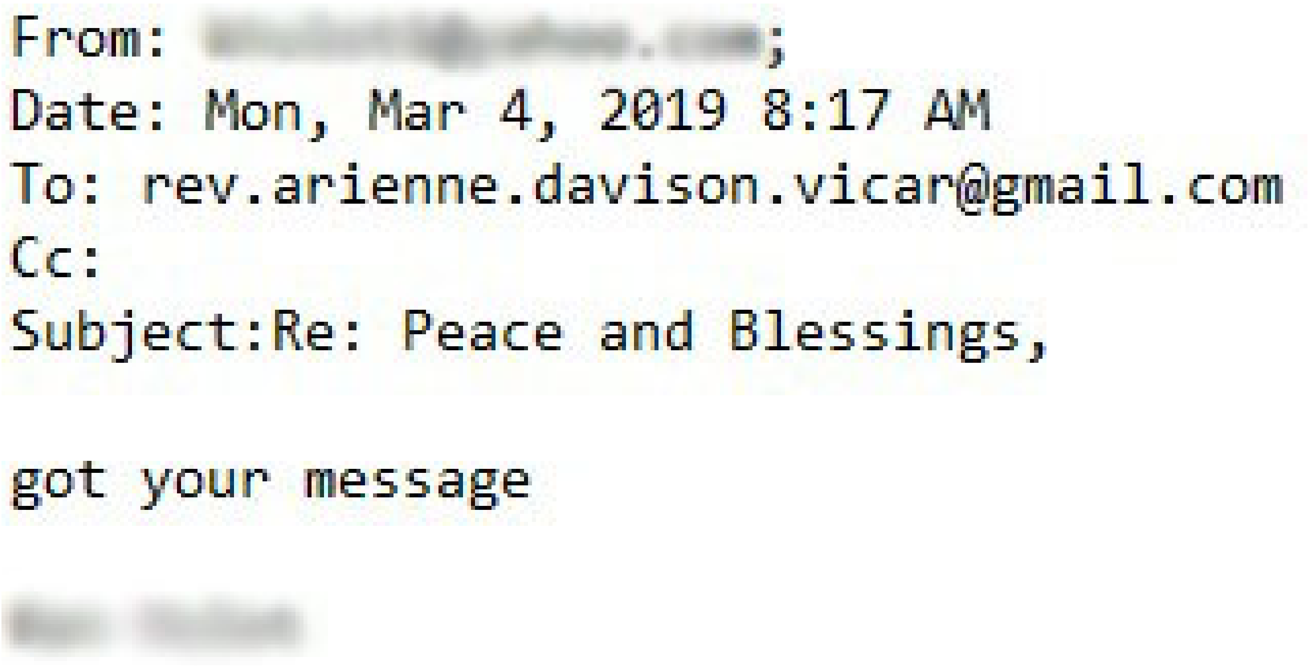
Hi [redacted]

Good morning and how are you?

I need a favor from you, please email me back when you get this message.

Peace and Blessings,

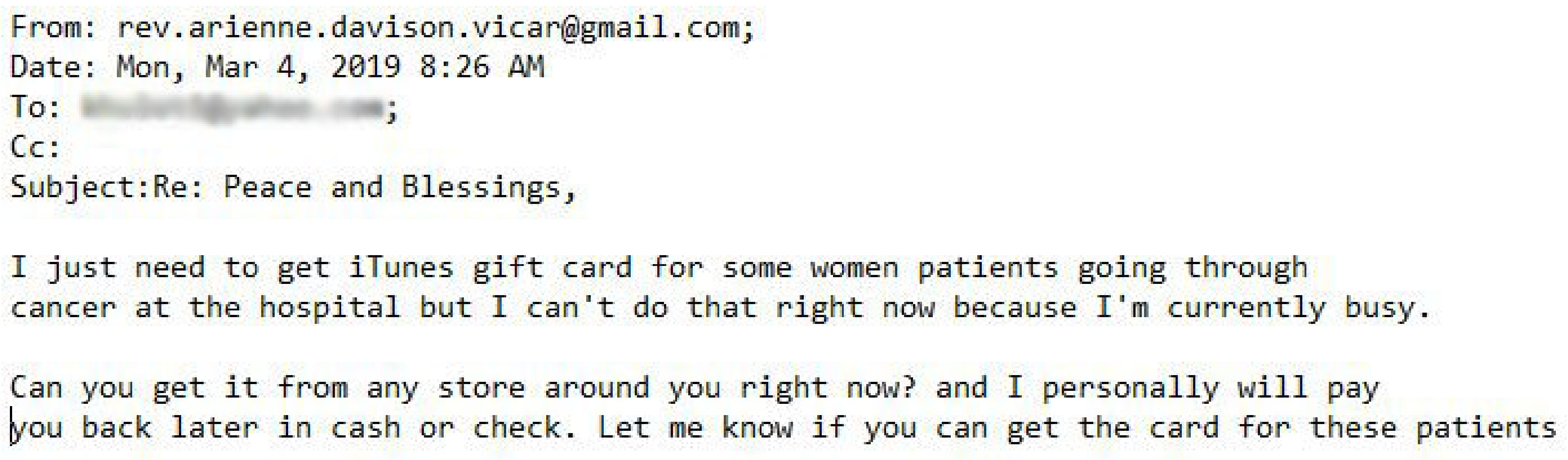
Rev.Arienne.Davison.Vicar
St. Bede Episcopal
ChurchPort Orchard, WA



From: [redacted];
Date: Mon, Mar 4, 2019 8:17 AM
To: rev.arienne.davison.vicar@gmail.com
Cc:
Subject:Re: Peace and Blessings,

got your message

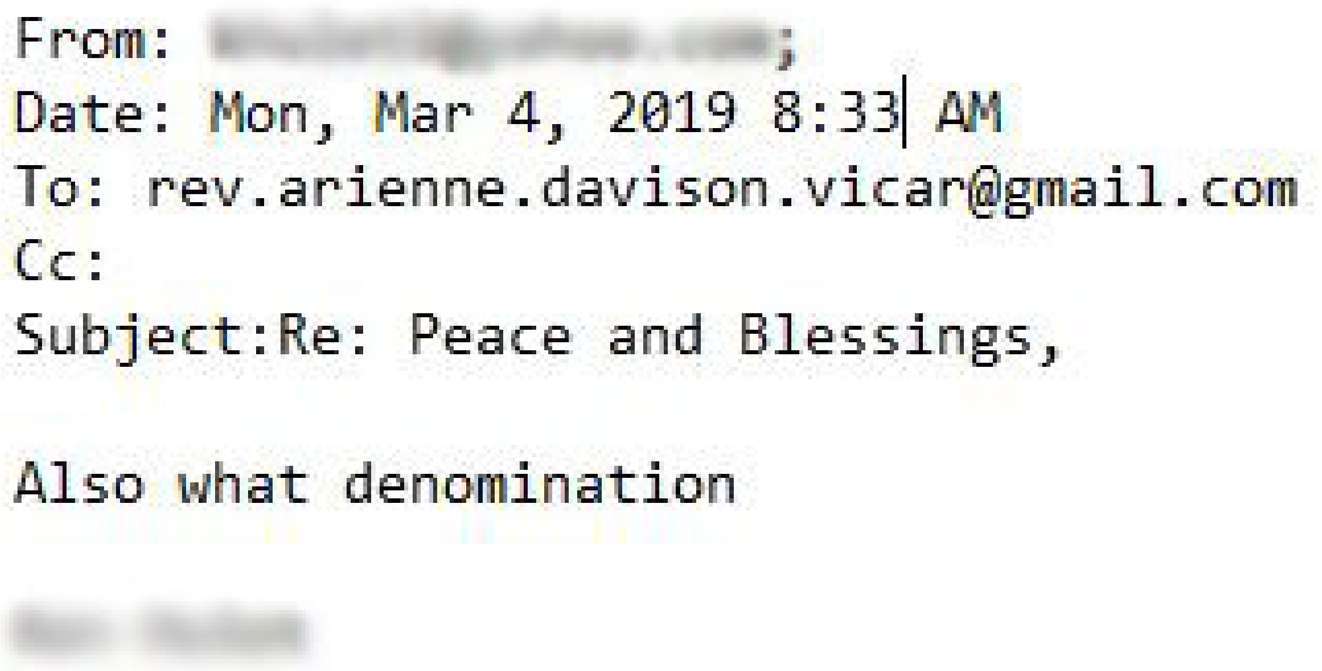
[redacted]



From: rev.arienne.davison.vicar@gmail.com;
Date: Mon, Mar 4, 2019 8:26 AM
To: [redacted];
Cc:
Subject:Re: Peace and Blessings,

I just need to get iTunes gift card for some women patients going through cancer at the hospital but I can't do that right now because I'm currently busy.

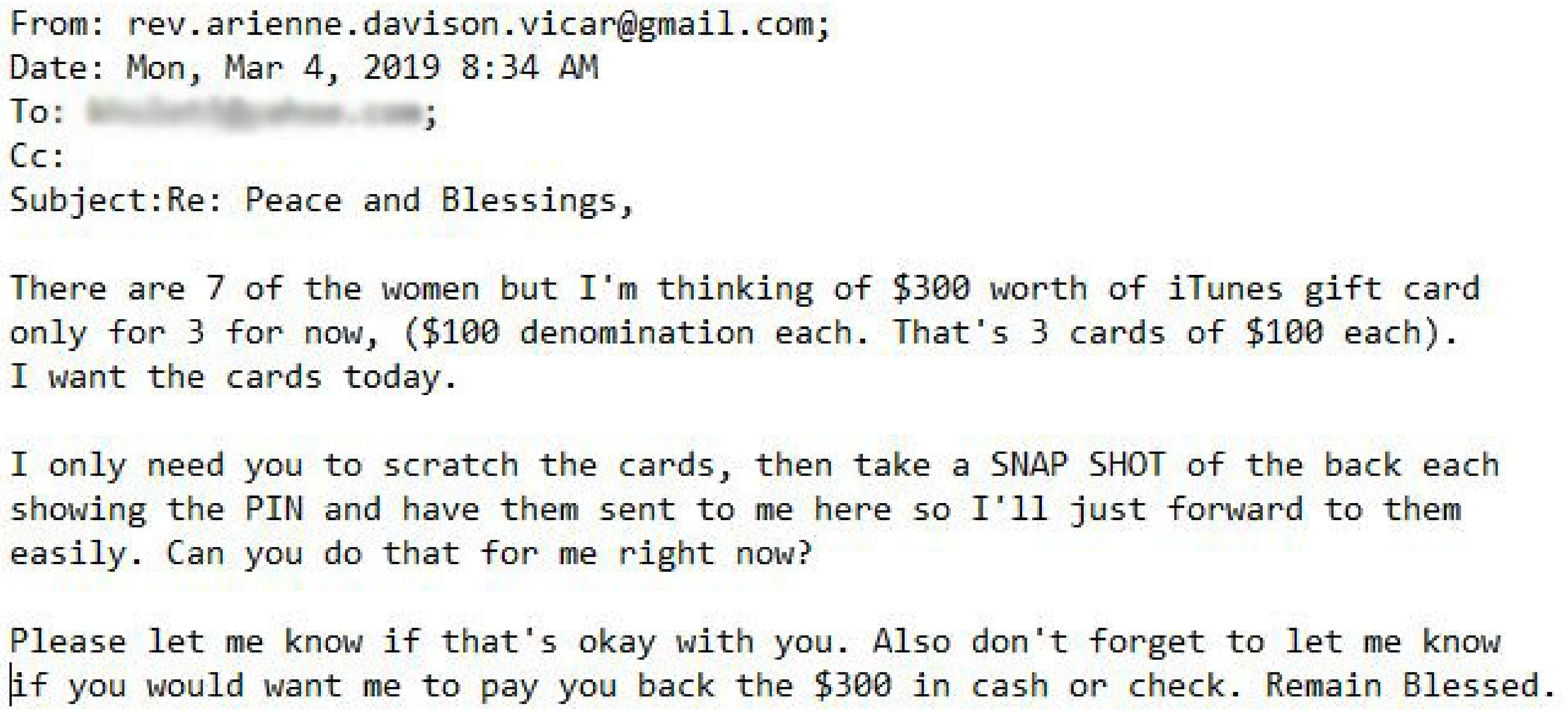
Can you get it from any store around you right now? and I personally will pay you back later in cash or check. Let me know if you can get the card for these patients



From: [redacted];
Date: Mon, Mar 4, 2019 8:33 AM
To: rev.arienne.davison.vicar@gmail.com
Cc:
Subject:Re: Peace and Blessings,

Also what denomination

[redacted]

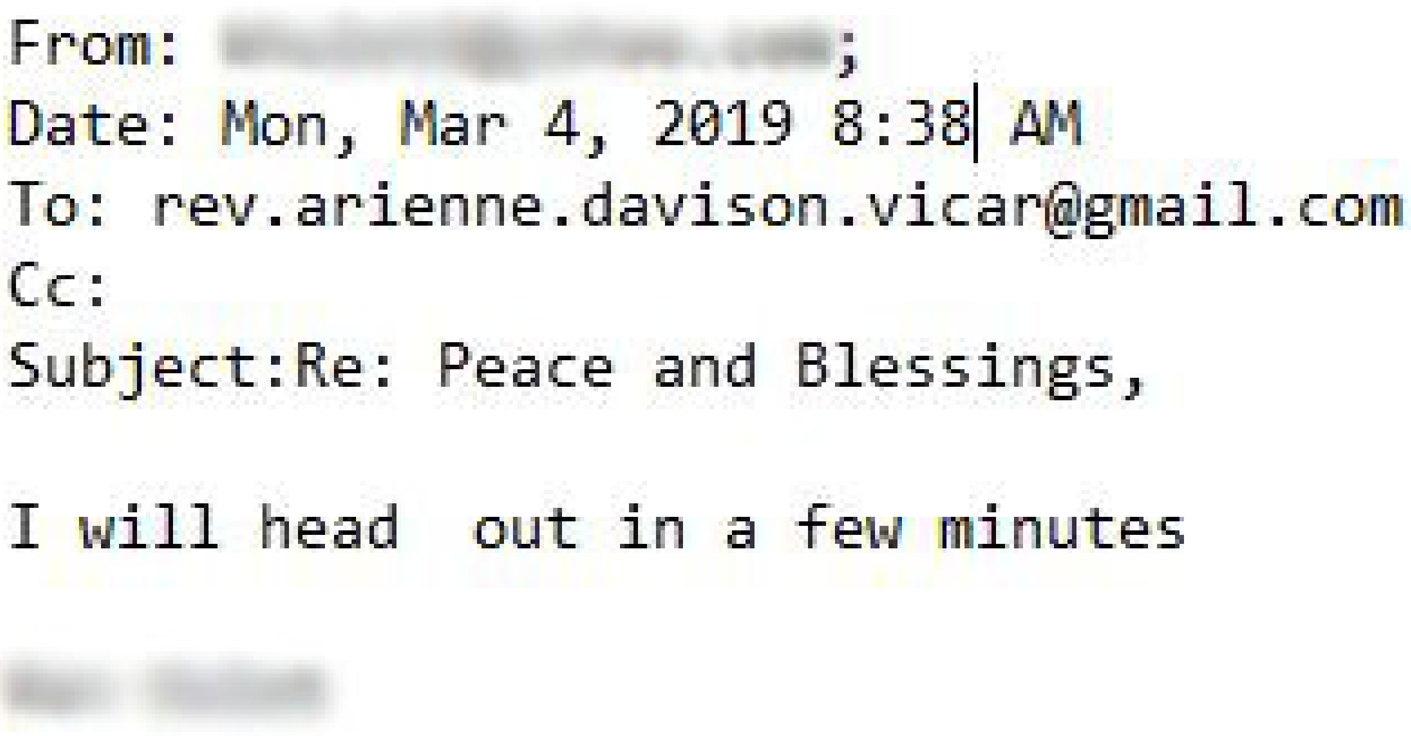


From: rev.arienne.davison.vicar@gmail.com;
Date: Mon, Mar 4, 2019 8:34 AM
To: [redacted];
Cc:
Subject:Re: Peace and Blessings,

There are 7 of the women but I'm thinking of $300 worth of iTunes gift card only for 3 for now, ($100 denomination each. That's 3 cards of $100 each).
I want the cards today.

I only need you to scratch the cards, then take a SNAP SHOT of the back each showing the PIN and have them sent to me here so I'll just forward to them easily. Can you do that for me right now?

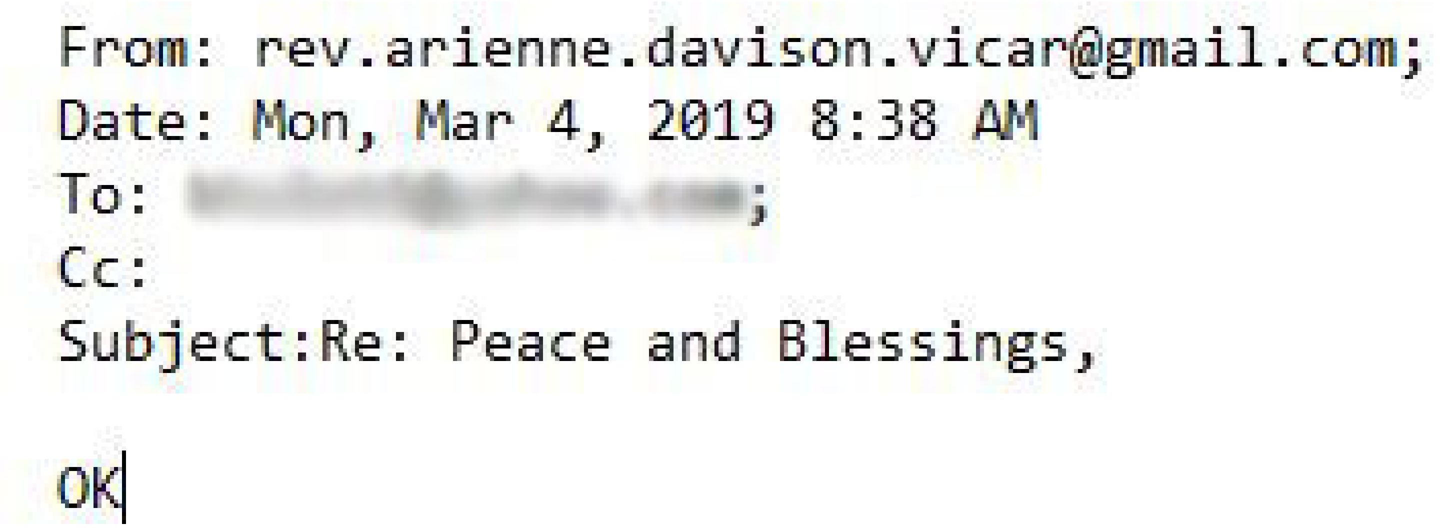
Please let me know if that's okay with you. Also don't forget to let me know if you would want me to pay you back the $300 in cash or check. Remain Blessed.



From: [redacted];
Date: Mon, Mar 4, 2019 8:38 AM
To: rev.arienne.davison.vicar@gmail.com
Cc:
Subject:Re: Peace and Blessings,

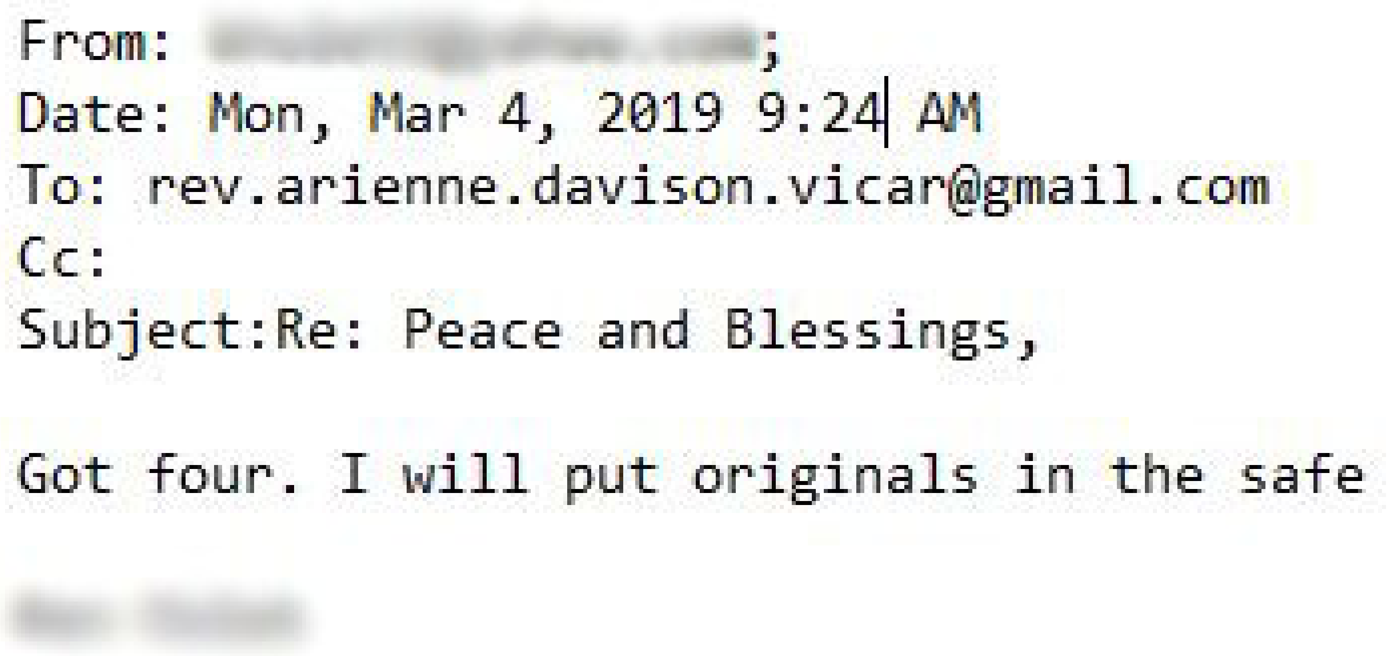
I will head out in a few minutes

[redacted]



From: rev.arienne.davison.vicar@gmail.com;
Date: Mon, Mar 4, 2019 8:38 AM
To: [redacted];
Cc:
Subject:Re: Peace and Blessings,

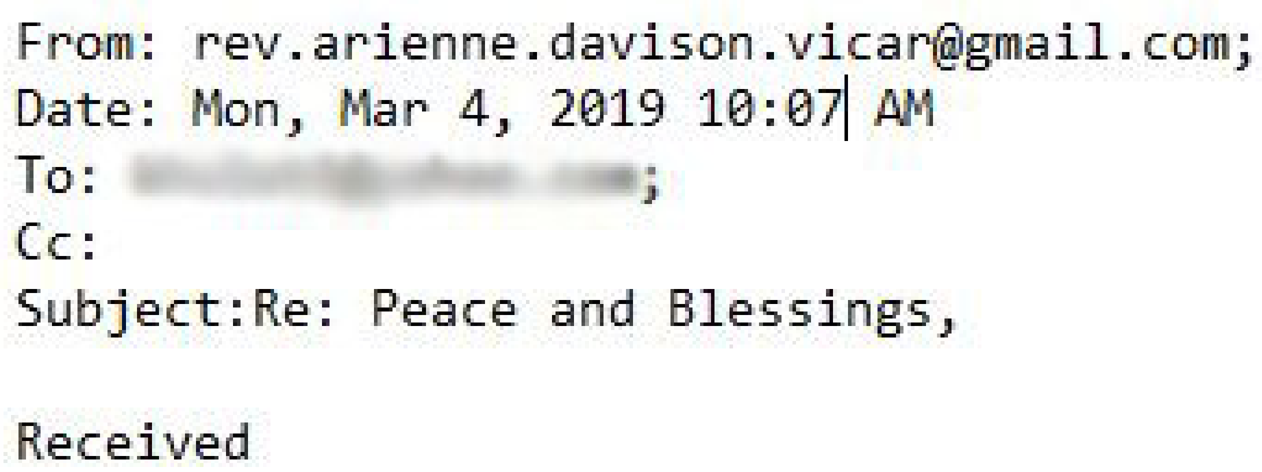
OK



From: [redacted];
Date: Mon, Mar 4, 2019 9:24 AM
To: rev.arienne.davison.vicar@gmail.com
Cc:
Subject:Re: Peace and Blessings,

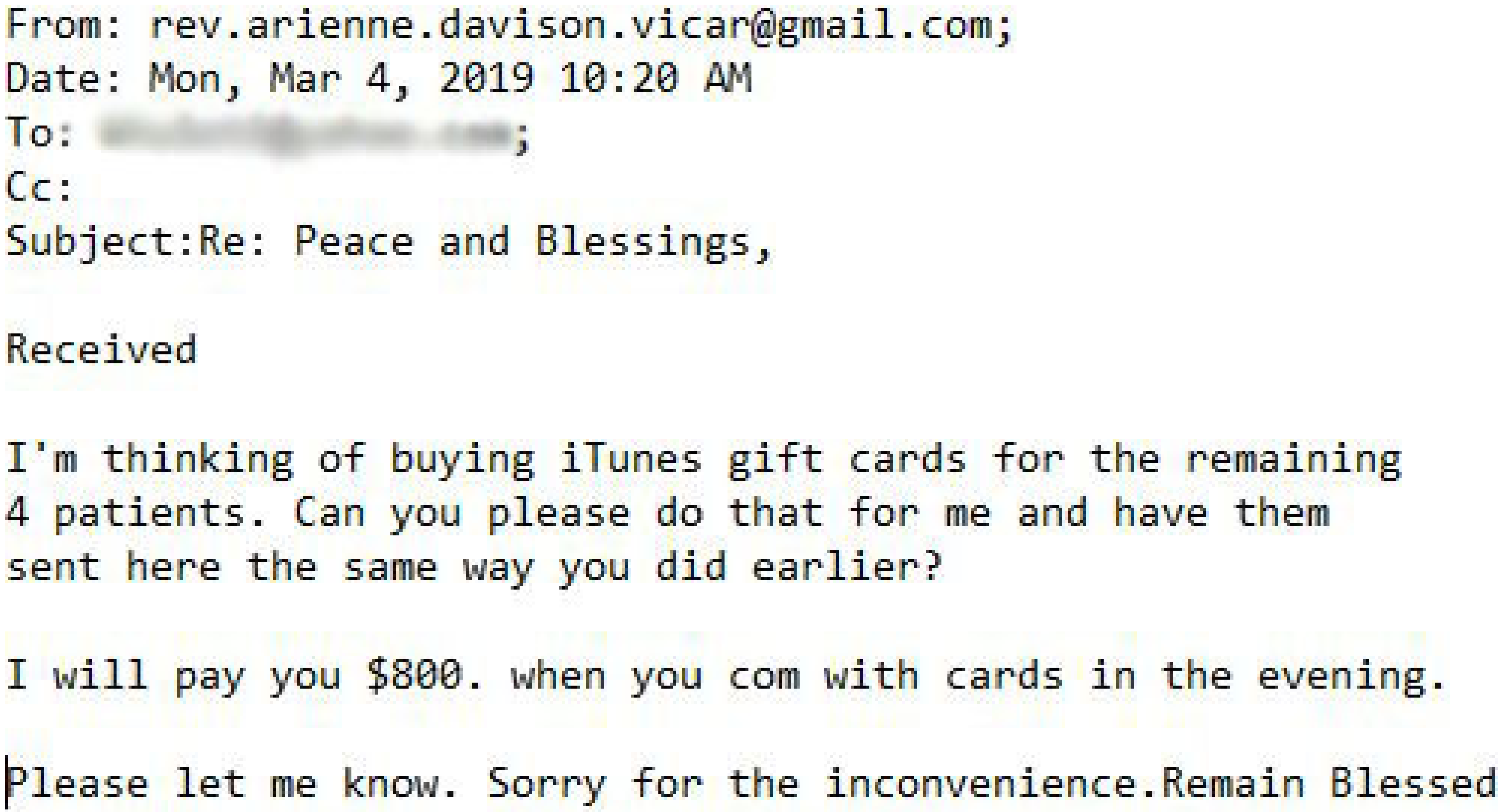
Got four. I will put originals in the safe

[redacted]



From: rev.arienne.davison.vicar@gmail.com;
Date: Mon, Mar 4, 2019 10:07 AM
To: [redacted];
Cc:
Subject:Re: Peace and Blessings,

Received



From: rev.arienne.davison.vicar@gmail.com;
Date: Mon, Mar 4, 2019 10:20 AM
To: [redacted];
Cc:
Subject:Re: Peace and Blessings,

Received

I'm thinking of buying iTunes gift cards for the remaining
4 patients. Can you please do that for me and have them
sent here the same way you did earlier?

I will pay you $800. when you com with cards in the evening.

Please let me know. Sorry for the inconvenience.Remain Blessed

This is not limited to email…

- **Voice Phishing** – Phishing by phone
  - Vishing is initiated by a caller
  - Just like email phishing, the caller may not be who they claim to be
  - It is easy to spoof Caller ID!

- **Smishing** – Phishing by text messaging
  - Asking for information, or sending a link, via text message
  - Example: Fake bank notifications
  - Don’t give out personal information in response to an incoming call or text
  - Verify the caller

Tips to Avoid Phishing

- Check who the email sender is.
- Check the email for grammar and spelling mistakes.
- Mouse over the link to see where it goes.
- Do not click the link – manually type it in.

Social Engineering

- Manipulation of people into divulging confidential or sensitive information
- Most commonly done over email, but also regularly carried out over the phone
- Can be a slow gain of information
- Can attempt to gain all information needed at once

Examples of Social Engineering

- Phone call targets employees at a business.
- Caller asks who the boss/CEO is.
- Requests his/her email address.
- Now the attacker has the username and the name of the person targeted for compromise.
- Social Media games and quizzes

Tips to Avoid Social Engineering

- Be careful with the information you disclose.
- Verify credentials of contractors.
- If you have any doubts on the identity of callers, hang up and call their official company number back.
- Don’t do polls or quizzes that ask for personal information

Password Safety

Protect Your Passwords

- https://howsecureismypassword.net/
- https://haveibeenpwned.com/
- Long = Strong (think passphrases)
- Use different passwords
- Don’t share passwords

Protect Your Passwords

- Multi-Factor Authentication
- Use a Password Managers

Protect Your Passwords

- Multi-Factor Authentication
- Use a Password Managers

Tips for Password Safety

- Utilize unique passwords across all websites/applications
- Enable and utilize 2FA on all websites that allow it
- Choose unique, non-true security questions

Internet Protection

Internet Protection Overview

- Search Engine Safety
- HTTPS
- Public Wi-Fi
- Internet of Things

Search Engine Safety

- Nowadays, users utilize search engines to ask every question they can think of.
- Users click on search results without first checking if it is a legitimate site.
- This happens commonly on social media websites as well.

Search Engine Safety

- Even if the website is reputable,
  the advertisement being displayed could
  be malicious and infect your computer or mobile device.
- Free things (music, movies, game cheats, etc.) are very commonly filled with malware, and are rarely what they say they are.

Tips for Search Engine Safety

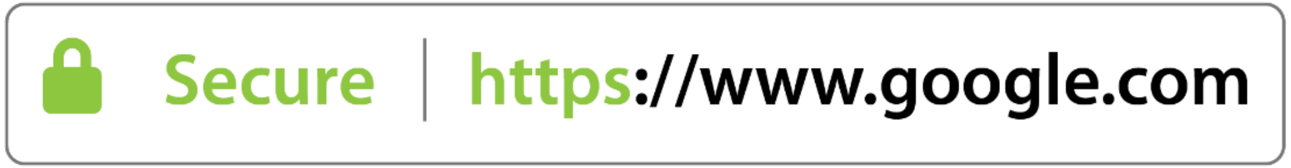
- Stick to click on sites on the first page of results
- Be careful when clicking on non-name recognizable sites
- Malware commonly masquerades as free things

HTTPS

HTTPS

- Is a protocol for secure communication over a computer network which is widely used on the internet

- HTTPS is typically notated by displaying a green lock in the web address bar



Secure | https://www.google.com

HTTPS

- No sensitive information should be typed into a page that is not secured by HTTPS.
- Even though a page is secured with HTTPS, it does not automatically mean the page is safe.
- Most browsers have begun to let users know more easily when they are on a non-secure page.

Tips for Secure Websites (HTTPS)

- Before entering sensitive information, check to see if the site is secured by HTTPS

- Check to make sure this is a reputable website before entering credit card information; don’t just depend on the HTTPS indicator

Public Wi-Fi

Public Wi-Fi

- Is a non-secure network that users can connect to for free

- Typically found in hotels, coffee shops, libraries and many other places

Public Wi-Fi

- Do not assume that a network named “Library” is actually the wireless network for the Public Library.

- Verify with the business owner the name of their network.

Public Wi-Fi

- Is very insecure, so you should treat every public Wi-Fi connection as compromised (unsafe).
- This means you should not utilize any sensitive websites when connected (banking, social networking, etc.)
- If you need to access one of these sites, utilize your cell phone and do not connect it to Wi-Fi, just use the cell service.

Tips for Public Wi-Fi

- Verify the Wi-Fi name with the business owner prior to connecting
- Treat public Wi-Fi connections as compromised (unsafe)
- Use VPN
- Utilize and anti-malware product to help prevent against cyberattacks while conected

Internet of Things

Internet of Things

- This type of internet connection is convenient, but opens up a security hole that needs to be secured.
- Examples of IoT devices include internet-connected thermostats and closed circuit cameras.
- If you can connect to it from anywhere, that means anyone can – by simply guessing your password.
- Disable any web features that you do not utilize.
- Make sure all IoT devices are kept up to date.

Internet of Things

- Routers are the first line of defense to protect IoT devices from exploitation.
- Routers should be immediately configured to change the default username and password to something unique.
- If someone gains access to your router they can see all other devices on your network.
- Make sure your router is regularly updated to avoid exploitation.

Tips for Internet of Things (IoT)

- Change default usernames and passwords on all devices including routers
- If you do not utilize the web features, disable them
- Make sure all IoT devices, including routers, are kept up to date with the newest firmware

Email Protection

Email Protection – 2FA

- Email is most important account needing protection, because if someone gains access to your email, they can utilize the password reset function to gain access to other services.

- As we mentioned earlier, 2FA is a great way to protect your email from being compromised.

Email Protection – 2FA

- Most major email providers allow you to set up 2FA with your email account.

- Once set up, the attacker would need your password and your cell phone in order to break into your email account.

Tips for 2FA and Email

- Password protect or utilize fingerprint reader to protect your 2FA app in case of a lost device
- Do not utilize SMS if you can help it as a 2FA method; always us an application orpush
- Enable 2FA not just on email but all critical websites and applications that allow it.

Password Reset

Email Protection – Password Reset

- When passwords are forgotten, the ability to reset your password is very convenient, but if not utilized properly this can allow someone to easily take over your account.

- Some websites do not require any security questions to be answered, nor require any additional information besides account email address to initiate a password reset.

Email Protection – Password Reset

- Usually when someone requests a password reset, an email is sent to the email address on file with this information.
- Monitor these emails and contact the vendor directly if you see these and did not initiate them yourself. (But remember the spam/phishing rules from earlier.)

Tips for Password Reset and Email

- Utilize strong unique passwords
- Utilize strong, not correct, security questions
- Monitor attempted password resets on your accounts for fraudulent activity

Spam Protection

Email Protection – Spam Protection

- Everyone gets spam; even with the best protection, some still slips through the cracks.

- Some email providers have better spam protection than others.

- A third party anti-spam product can supplement protection provided by the email provider.

Email Protection – Spam Protection

- Never open spam emails, even if you think it is funny to see the content inside.
- Never respond to spam emails.
- Be careful using your email address to sign up for contests or enter websites.
- When posting your email to a public website, always add special breaks in your email address. Example: ben(at)eset dotcom

Tips for Spam Protection and Email

- Utilize a different provider or 3rd party product if necessary
- Never click, open, or respond to spam messages
- When posting email to classified sites, us the following format to keep spam bots from retrieving and using your address: john.doe (at) email.com

Attachment Policy

Email Protection – Attachment Policy

- Attachments are one of the most common ways to get viruses or malware.

- Even though an attachment might look like a document or Excel file, it might contain a virus or malware.

Email Protection – Attachment Policy

- Never open attachments from unknown senders.
- If you see something that is questionable, send to your IT department for verification.

Tips for Attachment Policy and Email

- Never open or save attachments from an unknown sender
- Even though something looks like a file that you do not think is malicious, doesn’t mean it isn’t malicious

Preventative Measures

Secure Your Computer

- Use current anti-virus software
- Non-Admin accounts
- Stay up to date ("Patch, Patch, Patch!")

  (Windows, Browsers, Applications)
- Only install applications from trusted sources
- Don't leave unattended – Lock the screen

…and Secure your Mobile Devices

- Protect the device with a password
- If possible, use fingerprint authentication
- Disable unnecessary services
- Keep the OS and apps updated
- Enable “Find Your Phone” features
  - Remote Wipe
- Dangers of Public Wi-Fi
- Do not leave unattended

Essential Rules for Self Protection (thanks AARP!)

- Opt for electronic statements
- Buy a shredder
- Freeze your credit report
- Stop entering sweepstakes
- Stop giving out your SSN
- Credit Card vs. Debit Card
- Mobile payments
- National Do Not Call Registry

More Essential Rules

- Don’t answer unrecognized calls
- Be prepared to hang up
- Be wary of Public WiFi
- Watch what you share
- Don’t reveal your location
- Don’t fall for fear-based scams
- Don’t respond to scam-recovery pitches