# Protecting Your Identity Online

Michael DeVincenzo

Wyckoff Public Library

# Why is the Internet so vulnerable to attack?

- The world wide web was invented in 1993 by Sir Tim Berners-Lee. Why is the Internet still so vulnerable to attack?
- The Internet was originally called ARPANET, a so-called “network of networks” designed in the 1960s and 1970s to serve as a way to network computers across the country for the Department of Defense. Later, this was turned over to the academic world for further expansion in 1981.
- The Internet was designed as an open network of networks. It was assumed in its design that all actors and institutions using it would trust each other and be trustworthy.
- e-mail was invented as an open and trusted messaging system for ARPANET in 1971.

# Perspective: The Internet was built on a trusted user model

- Original paper email directory published in the early 80s had only 300 listed email addresses
- Most of those 300 people knew each other personally; many were colleagues and personal friends.
- If such a directory were to be published today, it is estimated it would be 72 miles thick.
- The creators of the Internet never anticipated, nor planned, for the mass adoption of the Internet and email by the general global public.

# Tip #1

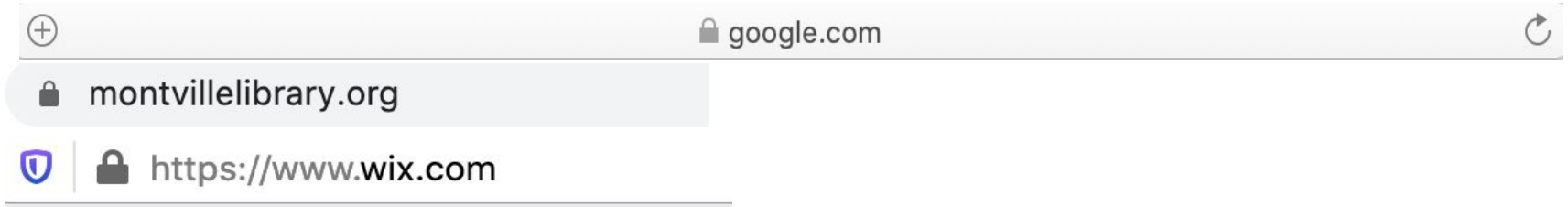
- Strong passwords (I know, everyone hates passwords, especially strong ones)
- Weak password example: Mcduff13
- Strong password example: CP\g6$+8H5zx3b;)
- Method #1: Password Manager (1Password, Lastpass, Keeper)
- Method #2: Random Password Generator
- Method #3: Alliterations and Memorable Random Phrases
- Resources:

https://www.security.org/how-secure-is-my-password/

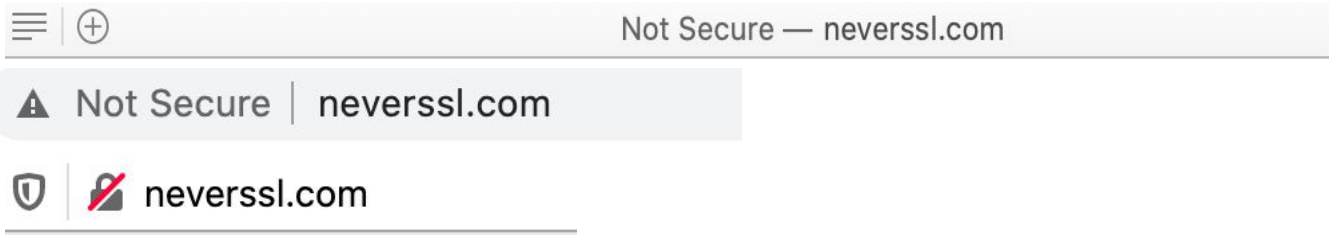
https://www.pcmag.com/picks/the-best-free-password-managers

# Tip #2

- Look for the lock (https vs http)




VS.



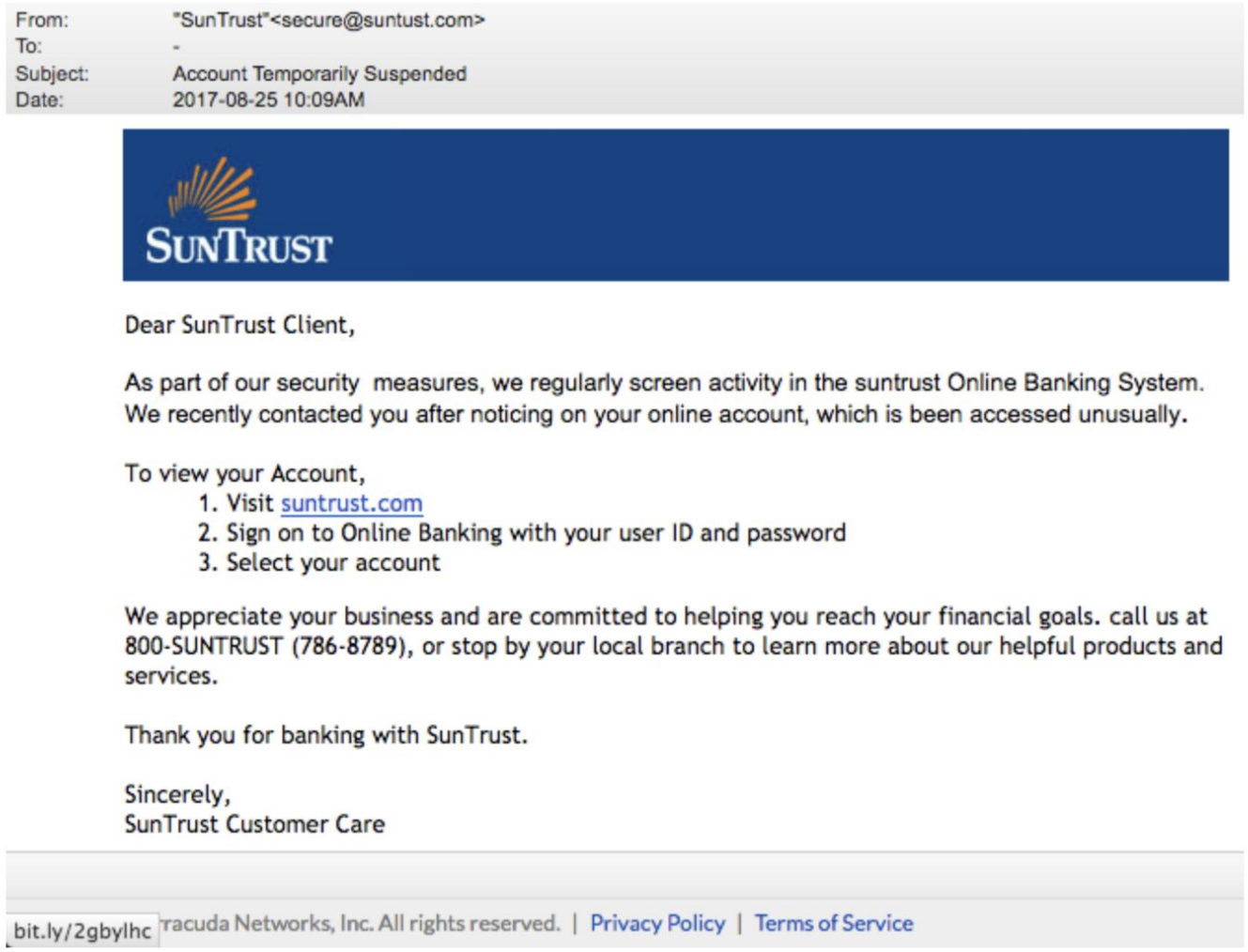
# Tip #3: What is Phishing? How can I avoid it?

- How to spot phishing emails:
- Grammatical Errors
- Low Resolution, old, or inaccurate logos
- Odd URL (web address) in link
- From an odd email address

# Tip #4: What is Smishing? How can I avoid it?

- How to spot smishing text messaages:
- Be wary of unsolicited, out of the blue contact — “Fraudulent activity detected”
- Spelling and grammatical errors
- If concerned, contact business/service provider DIRECTLY.
- Report fraudulent texts to your wireless carrier by forwarding the text to 7726

# Phishing Example #1



From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

SUNTRUST

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

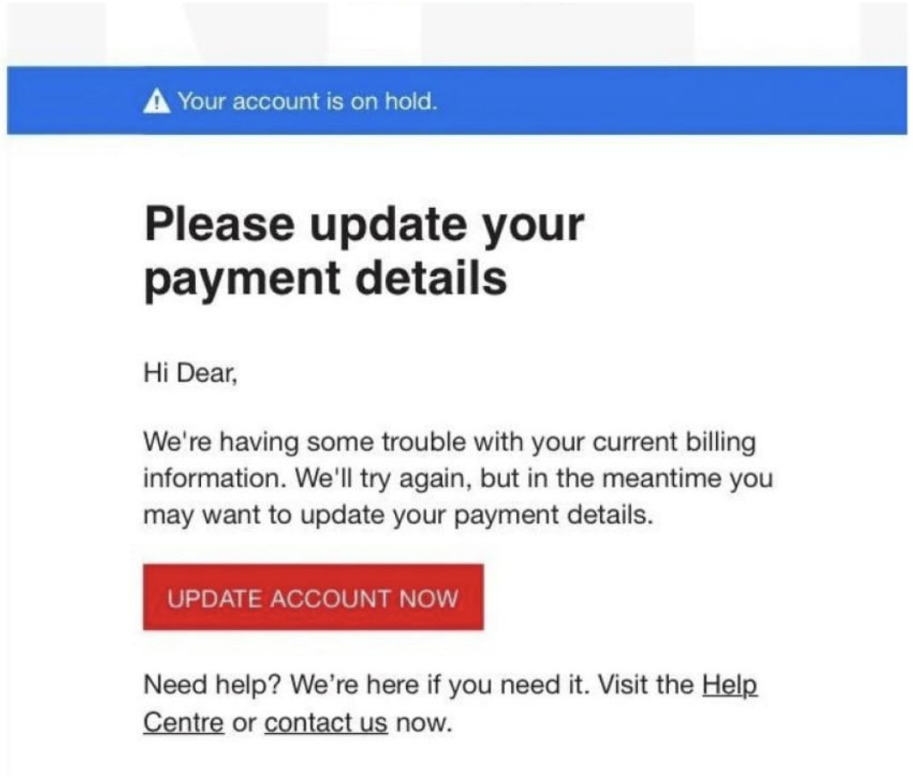
We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

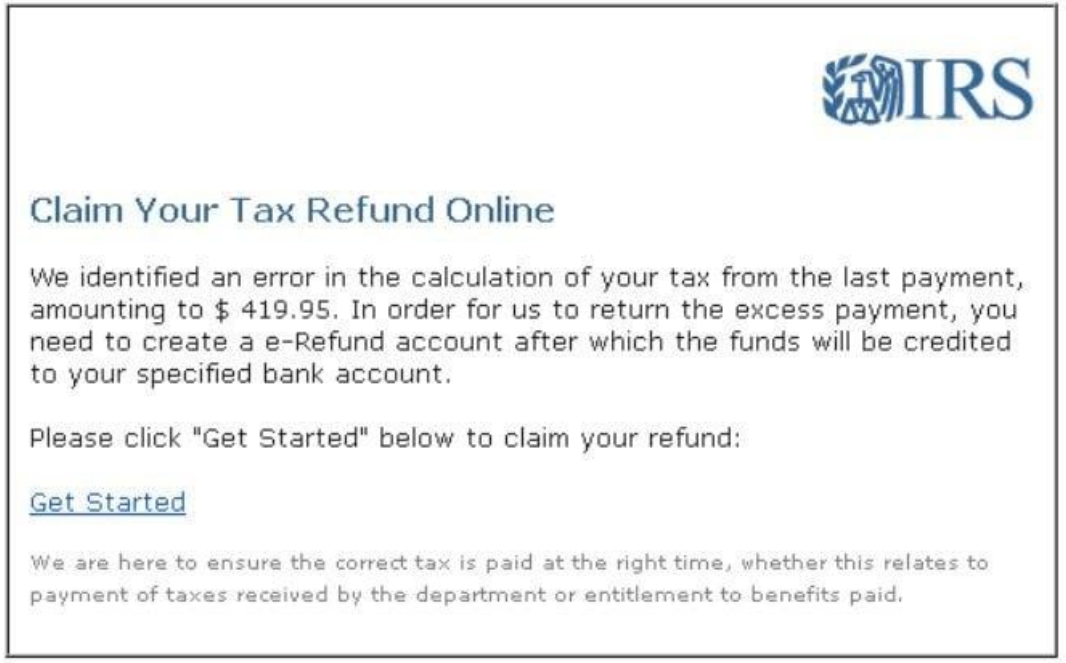
Sincerely,
SunTrust Customer Care

bit.ly/2gbylhc racuda Networks, Inc. All rights reserved. | Privacy Policy | Terms of Service

# Phishing Example #2



# Phishing Example #3



IRS

Claim Your Tax Refund Online

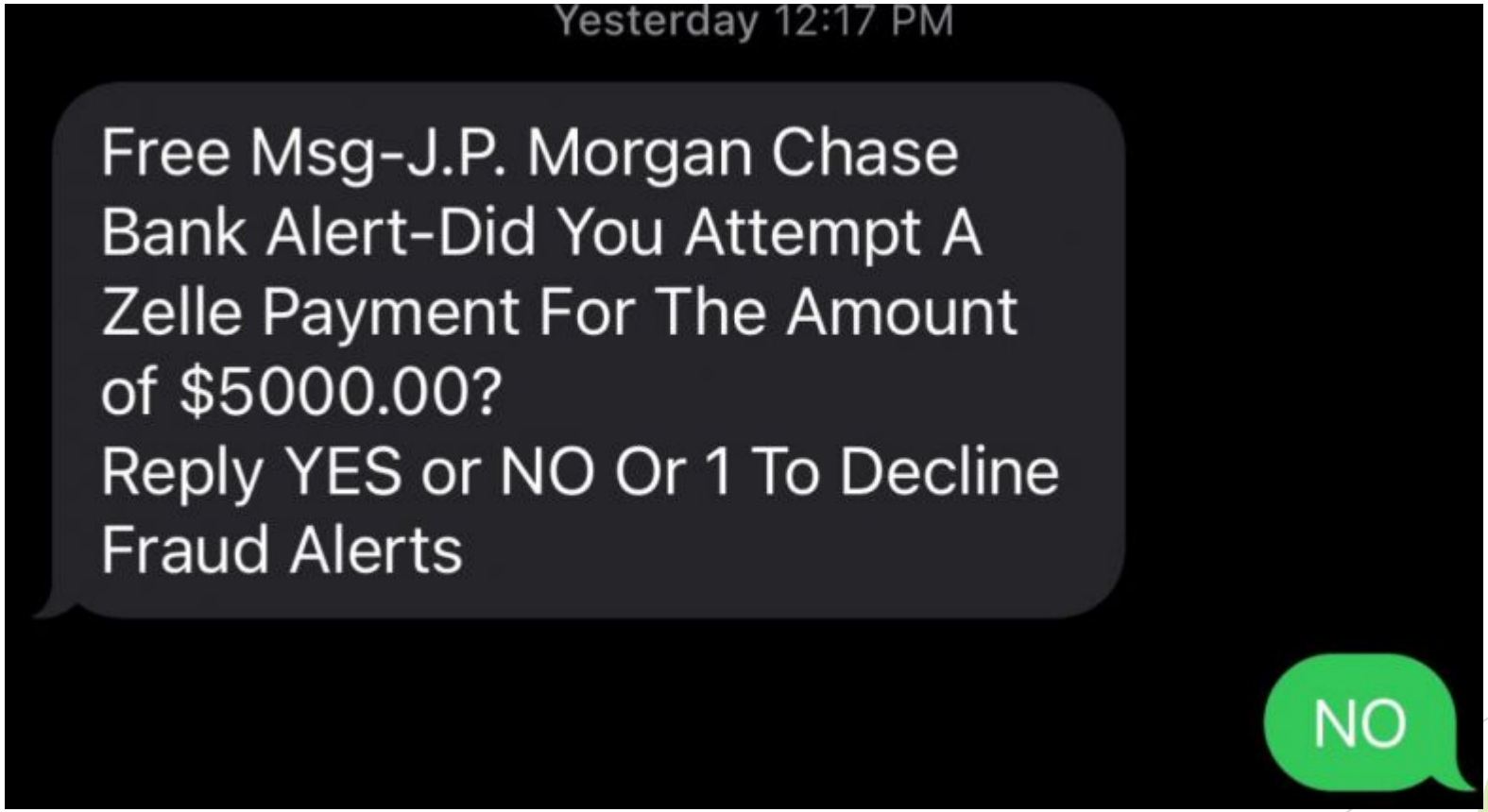
We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

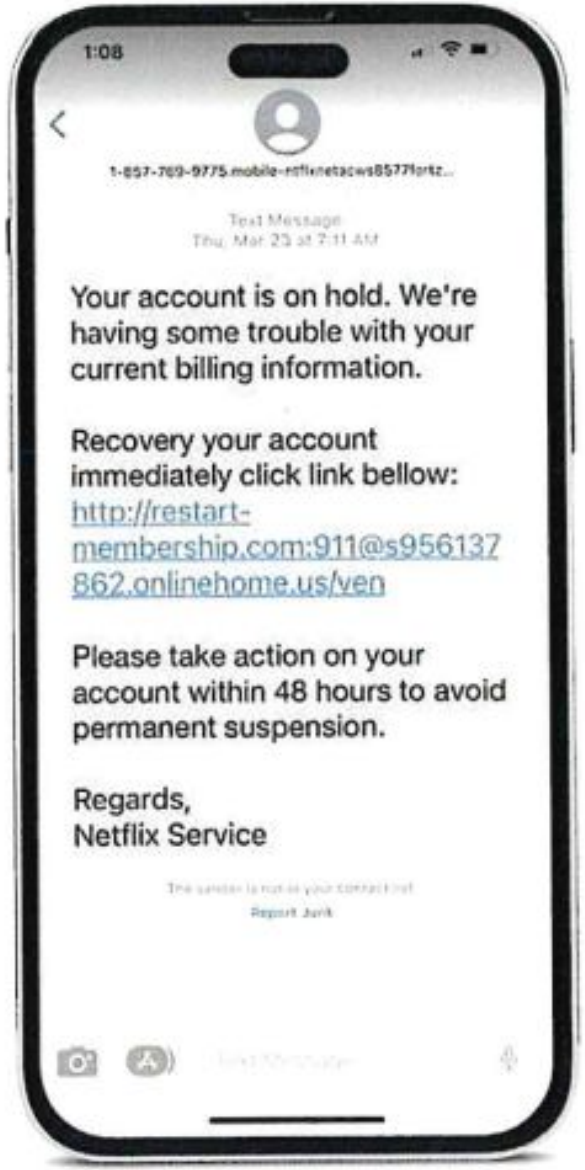
Get Started

We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

# Smishing Example #4



# Smishing Example #2



# Malware – What is it? How Can I avoid it?

- Malware is software that is designed to damage your computer, pure and simple.
- Strategies to avoid it:
- 1. Avoid downloading pirated content on the Internet
- 2. Avoid downloading free software from untrustworthy sources
- Use tools like Malwarebytes to periodically scan your computer for malware
- Resources:
- https://www.malwarebytes.com
- https://www.mcafee.com/en-us/antivirus/malware.html

# Malware Example #1: Computer Virus

- Computer viruses are most often transmitted as email attachments. Never open email attachments from untrusted or unknown sources.
- Be skeptical of that appear to be from people you know but are actually "spoofed" Check this by examining not just the name attached to the email, but the actual email address that is sending you the message
- Jane Smith (jsmith@gmail.com) vs. Jane Smith (j3287542937smith@gmail.com)
- Example: the "ILOVEYOU" virus caused $10 billion dollars in damage
- Not that common of a threat currently

# Malware Example #2: Ransomware

- Ransomware is a kind of malware that encrypts the files on your computer, preventing you from using it.
- The malware will ask for payment of a ransom by a deadline, or your computer will be erased and your files lost. The ransom will typically be requested in a cryptocurrency.
- Strategies:
- 1. Always keep a backup of your computer to have a safe copy you can restore later
- 2. Keep your operating system software up to date
- 3. Be wary of clicking on direct links in emails or from social media networks.

# Ransomware Example: WannaCry (North Korea 2017)

# Why Can't They Catch These Guys??

- Hacking and Identity Theft is a global problem.
- Bad actors often operate out of nations that are beyond the reach of the US/Interpol. (Iran, Russia, China, North Korea, etc.)
- Hackers are very skilled and sophisticated in their methods of avoiding detection.
- State sponsored hackers are even harder to detect.
- It is estimated that 95-96 percent of cybercrime is unsolved.
- The sheer volume of attacks is overwhelming


FIREEYE
Customer Stories
Blogs
Search FireEye.com
Solutions
Services
Partners
Support
Resources
Company
[X] NEW ATTACK: FROM [JORDAN] TO [CHILE]
[X] NEW ATTACK: FROM [ALGERIA] TO [SAUDI ARABIA]
[X] NEW ATTACK: FROM [PORTUGAL] TO [THAILAND]
LOCAL TIME
9:13:14
ATTACKS TODAY
280434
FIREEYE CYBER THREAT MAP
LATVIA
PORTUGAL
ALGERIA
EGYPT
JORDAN
SAUDI ARABIA
THAILAND
COLOMBIA
ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)
Powered by FireEye Labs
TOP 5 REPORTED INDUSTRIES [PAST 30 DAYS]
FINANCIAL SERVICES
SERVICES/CONSULTING
TELECOM
MANUFACTURING
INSURANCE
VIEW FULL SCREEN
The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy

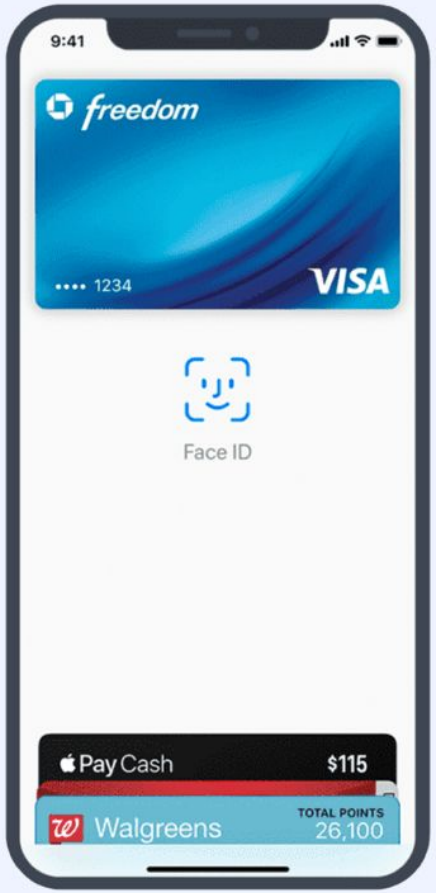
# What else can I do to stay safe?

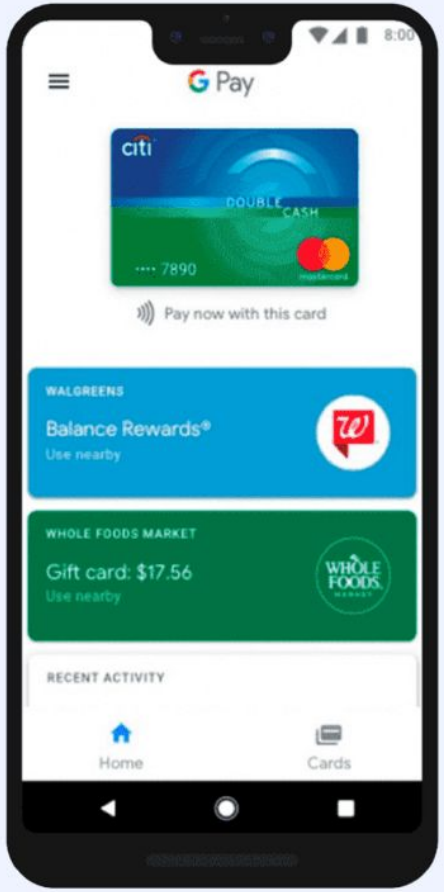
- Digital Wallets
- Only use Venmo/Zelle with trusted people known to you personally and double check the username of the recipient!
- Paperless billing
- Automatic updates ON

# What else can I do to stay safe (cont)?

- Slow down, stay calm
- Think about what you share on social media (favorite bands, birthday, etc)
- Delete old accounts you no longer use
- Use Multifactor Authentication

# Digital Wallets




soft journ

# Tap to Pay


Resource: 3 Reasons Why You Should Tap to Pay

# Wrap-Up

- The best defense against computer attacks is not technical, it is an attitude and approach to using the Internet
- The Internet by its nature is designed to be an open network of trusted people. It will always be vulnerable.
- Use password managers or generators. Don’t reuse the same password over and over again.
- Beware of clicking on links in emails or on social media even supposedly from people you trust.

# A Final Word…