



CENTER[™]
for Cyber Safety
& Education

**Safe and Secure
Online**

**Building a global
cyber community *for
good.***



Who We Are and What We Do

The Center for Cyber Safety and Education

- Charitable foundation of ISC2*, a leading nonprofit member organization for cybersecurity professionals
 - * *ISC2 = International Information System Security Certification Consortium*
- Educates the public on cyber safety practices
- Raises awareness of cyber career options
- Provides cybersecurity scholarships and support
- Assists small organizations with cyber risk



Agenda

- How Vulnerable Are We?
- Basics of Being Safe and Secure Online
 - Passwords
 - Wi-Fi
 - Firewalls
 - Virtual Private Networks
 - Secure Websites
 - Email
- Malware, Phishing and Ransomware
- Social Media
- Protecting Our Families
- Home Safety
- Summary
- Additional Resources

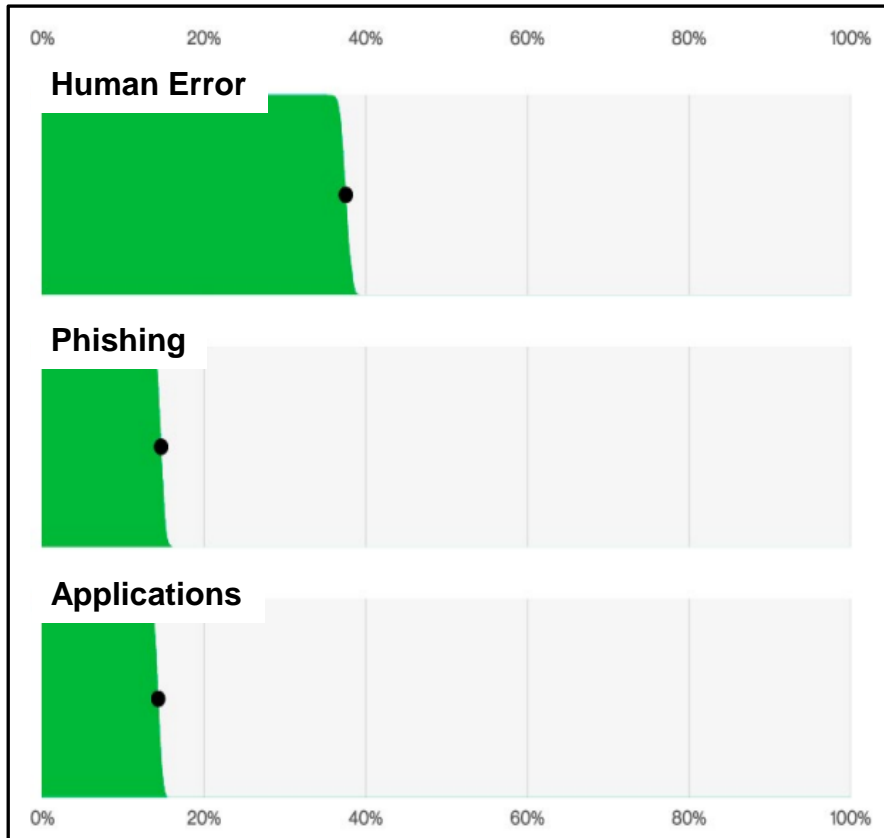
How do you and your family use the Internet?

- Connect with other people
- Shop and access bank information
- Watch movies and play games
- Use social media
- Online classes, webinars, podcasts



How Vulnerable Are We?

Verizon 2024 Data Breach Investigations Report



- *90% of breaches involve a human element or error*
- *Surveys indicate that over 70% of adults admit taking risks such as sharing passwords*
- *85% of attacks start with phishing emails*
- *Median time to click on a malicious link after opening email is 21 seconds, with additional 28 second to enter their data*
- *Equals less than 60 seconds for users to fall for phishing emails*
- *180% increase in exploitation of application vulnerabilities from 2023!*
- *Stems from Ransomware*
- *Median loss is \$46,000 per incident, ranging from \$3 to Millions*

Basics of Being Safe and Secure Online

Safe Passwords!



Did you know?

- *53% haven't changed password in 12 months*
- *57% write them on sticky notes*
- *62% share passwords over email or text*
- *44% recycle passwords across business and personal accounts*

Safe Passwords!

- Change passwords at least every 30 to 90 days
- Don't write passwords down, especially on media that is close to your devices
 - *Use a password vault or manager: NordPass, 1Password, KEEPER, RoboForm, LastPass, etc.*
- Don't share passwords
- Don't recycle/reuse passwords, especially between personal and business accounts
- Don't use commonly used passwords or words from your social media account
- Make it a phrase - the longer the better (IEat@2OnTuesdays instead of Eating2!)
 - *12 character minimum with no repetitive or sequential characters*
- Use multi-factor authentication whenever offered, or set it up
 - *Something you know (password, PIN)*
 - *Something you have (phone, USB key)*
 - *Something you are (fingerprint, face)*
- Make sure passwords are used on all mobile devices and computers



Public Wi-Fi

There are risks of connecting to Wi-Fi at your local coffee shop, airport or hotel

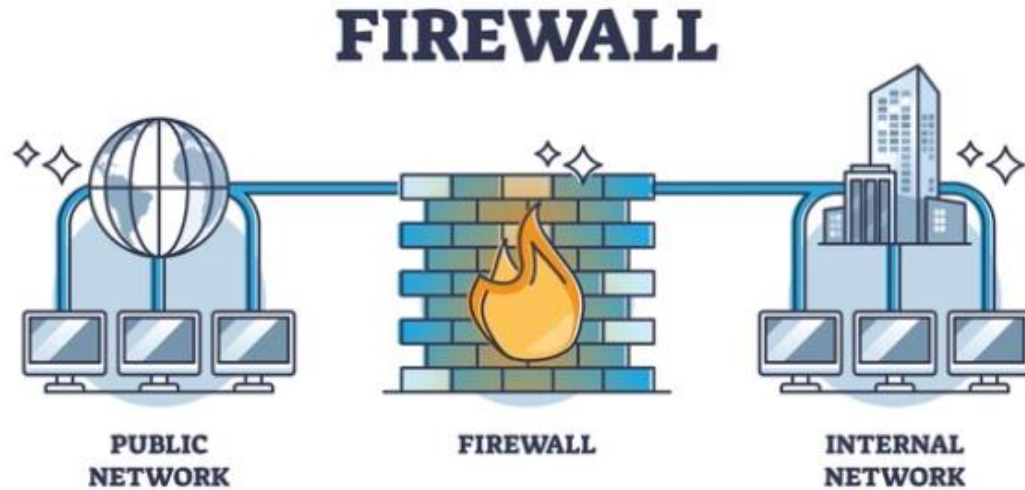
Avoid anything you do not have to do right then:

- Do not check your bank information
- Make purchases or online transactions at a later time if possible

If you do have to connect:

- Connect with caution
- Double check that you are connecting to the correct network

Firewalls



“Walls around a castle”

- Most Operating Systems include one – may need to configure on Apple devices
- Software version can be purchased from software vendor or Internet Service Provider (ISP)
- Prevents unauthorized access through a series of configured rules
- Make sure yours is on and updated
- Buy an external hardware firewall, especially if your device does not have a software version
 - Positioned between computer and Internet
 - Some ISP routers include firewalls

<https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use>

Virtual Private Network (VPN)

- Encrypted tunnel between a device and a remote network
- Protects entire device; Hides identity and browsing activity
- Private: A remote device acts as if it is directly connected to the network
- Most commercial entities have one
- There are subscriptions for home use
- NordVPN, Surfshark, Norton, TOTALVPN, etc.

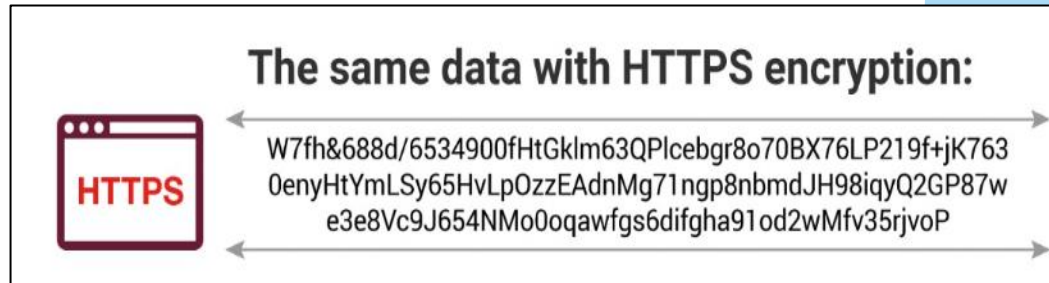
<https://us.cybernews.com/lp/best-vpn-us>



Is this Site Secure?

Look for the “S”

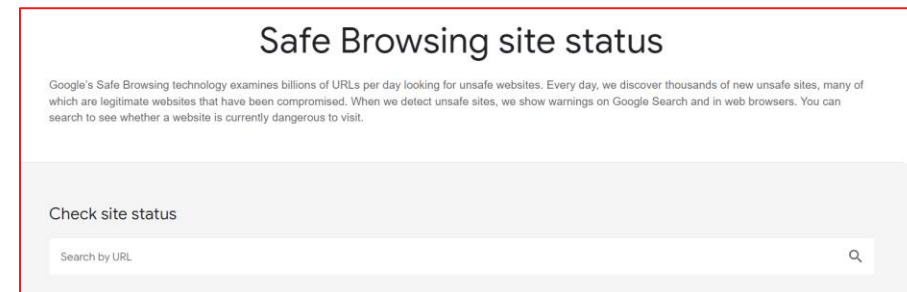
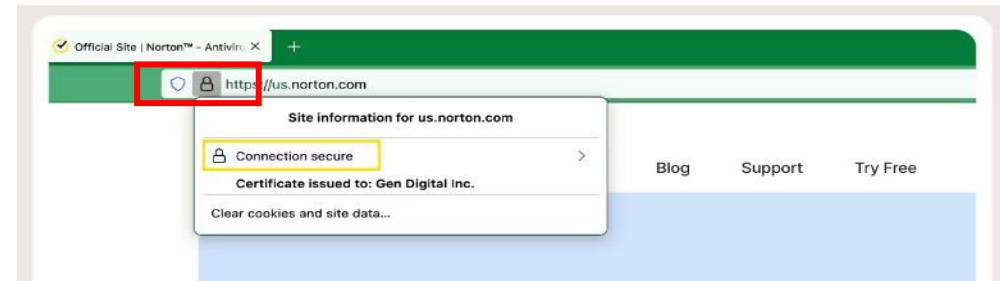
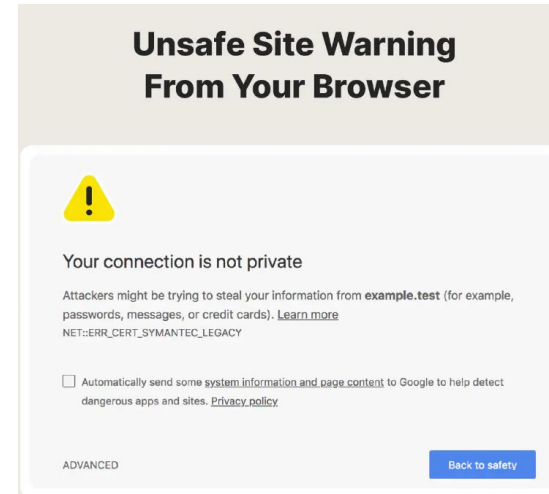
- http: **H**ypertext **T**ransfer **P**rotocol
- https: **H**ypertext **T**ransfer **P**rotocol **S**ecure
- http and https transfer data between servers and devices
- https adds a security layer that encrypts the data
- Essential for banking, healthcare, etc.



- ***But.....A Hacker can still redirect you to a different site through “Domain Name System (DNS) Spoofing”***
- ***He will force your browser to his website, which will often look like the original site (often with errors)***
- ***Use other security measures to reduce the chances that this will occur (No Public Wi-Fi, VPN, other technologies)***

Is This Site Secure?

- Site might indicate it is unsafe
- Lock on the far left side of the address bar
- Website safety check
<https://transparencyreport.google.com/safe-browsing/search>
- Beware of “typosquatting”
 - Someone bought domain similar to a well-known site such as google.com
 - Mistype google.com and end up on a fake site with malware
- Your tools will flag issues
 - Norton, Bitdefender, Malwarebytes, etc.



Personal vs. Work Email

- Work email is important for conducting business
- It is not the safest way to send personal information
- Any email sent or received on your work email is owned by your organization
- Also, when you leave an organization, you relinquish your work email address
- Use your personal email for all non-work-related emails. This includes (but is not limited to):
 - Communications with friends and family
 - Health care matters
 - Loyalty programs (airline, hotel, etc.)
 - Bills, credit card statements, banking information



The M, P, Rs of Threats

Malware, Phishing, Ransomware – What Are They?

Malware

- Software used by bad actors to steal your information
- Often installed by getting you to click a link or open an attachment
- Can also be installed by giving someone remote access to your computer

Phishing

- Steals your information by getting you to click a link, download a document, or perform an action
- Usually through email
- Often looks like a real email from a company you do business with

Ransomware

- A type of malware that locks up your information until you pay a ransom to restore it
- Could hold your photos, personal information, or other documents
- Beware! 56% of companies pay the ransom; 46% recover data fully

Malware, Phishing, Ransomware

30%

Increase in
Malware from
2023

85%

Attacks Start
with Phishing
Emails

5,600

Ransomware
Incidents
Reported since
2023

560,000

New Malicious
Applications
Per Day

94%

Malware/
Ransomware
Originate via
Email

264%

Increase in
Healthcare
Ransomware
Attacks in 5 years

Malware – How to prevent it

Get an anti-virus system and keep it updated!

Run updates on your:

- Operating system
- Internet browser
- Software
- Anti-virus system
- Tablets
- Mobiles



Only use reputable sites (and double check the URL) for any downloads

Clear your browser cache occasionally

Delete out-of-date or unused applications

Do not give anyone access to your computer



Phishing – How to Prevent it

- Never click links, open attachments or follow instructions from unknown or untrusted sources
- Never send sensitive information through e-mail
- If you get an out-of-character or unexpected email from someone, check with them before taking action
- Log out when you are finished, especially if you are using a shared or public computer


Gift Card Scam

Redeem your free \$50 Visa Gift Card

Richard Moore <visagiftcards@gmail.com>
TO: Fisikin, Ken
Tue 3/29/2022 4:08 PM

You have been randomly chosen to be the recipient of a **free \$50 Visa card**. Use your mobile device to scan the QR code below, and you will be directed to a web site that contains a one minute survey with simple instructions on how you can redeem your free card.

Please hurry though, as this exclusive offer will expire in three days. Visa cards can be used at 44 million merchant locations in more than 200 countries and territories.



What are they?

Offers of gift cards, gifts, special access, etc.

The "bad actor" is trying to get you to click something, enter information, and/or scan a QR code.

They contain:

- High sense of urgency
- Something that is too good to be true
- Requests for sensitive information

Delete them! Contact the company directly if you think you actually won something.

Fake Invoice Scam

From: xero [mailto: [REDACTED]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [REDACTED]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for \$373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit <https://fn.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN>.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks

NJW Limited



- Relies on fear and urgency
- Asks for payment for goods never ordered or received

Advance Fee Scam

Naomi Surugaba [azlin@moa.gov.my]



Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,

I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.

I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.

Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US\$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.

I am here seeking for an avenue to transfer the fund to you in only you're reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent s and I want you to help me transfer the fund into your bank account for investment purpose.

Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your

country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.

Remain blessed,

Miss Naomi Surugaba.

- Foreigner preying on emotions
- Offers money in exchange for bank details

PayPal Scam

Attention! Your PayPal account will close soon!

Dear Member,

We have faced some problems with your account Please update the account .If you do not update will be Closed.

To Update your account, just confirm your informations.(It only takes a minute.)

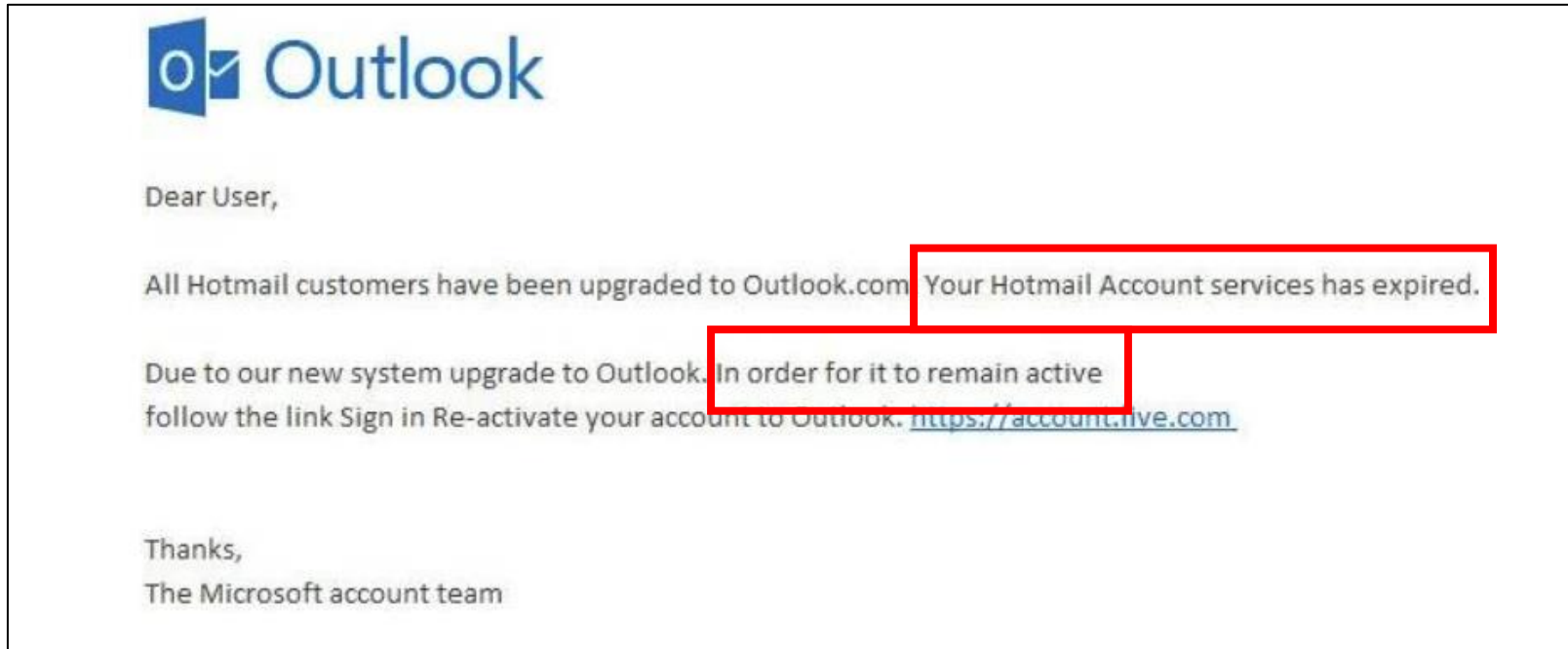
It's easy:

1. Click the link below to open a secure browser window.
2. Confirm that you're the owner of the account, and then follow the instructions.

Relog in your account now

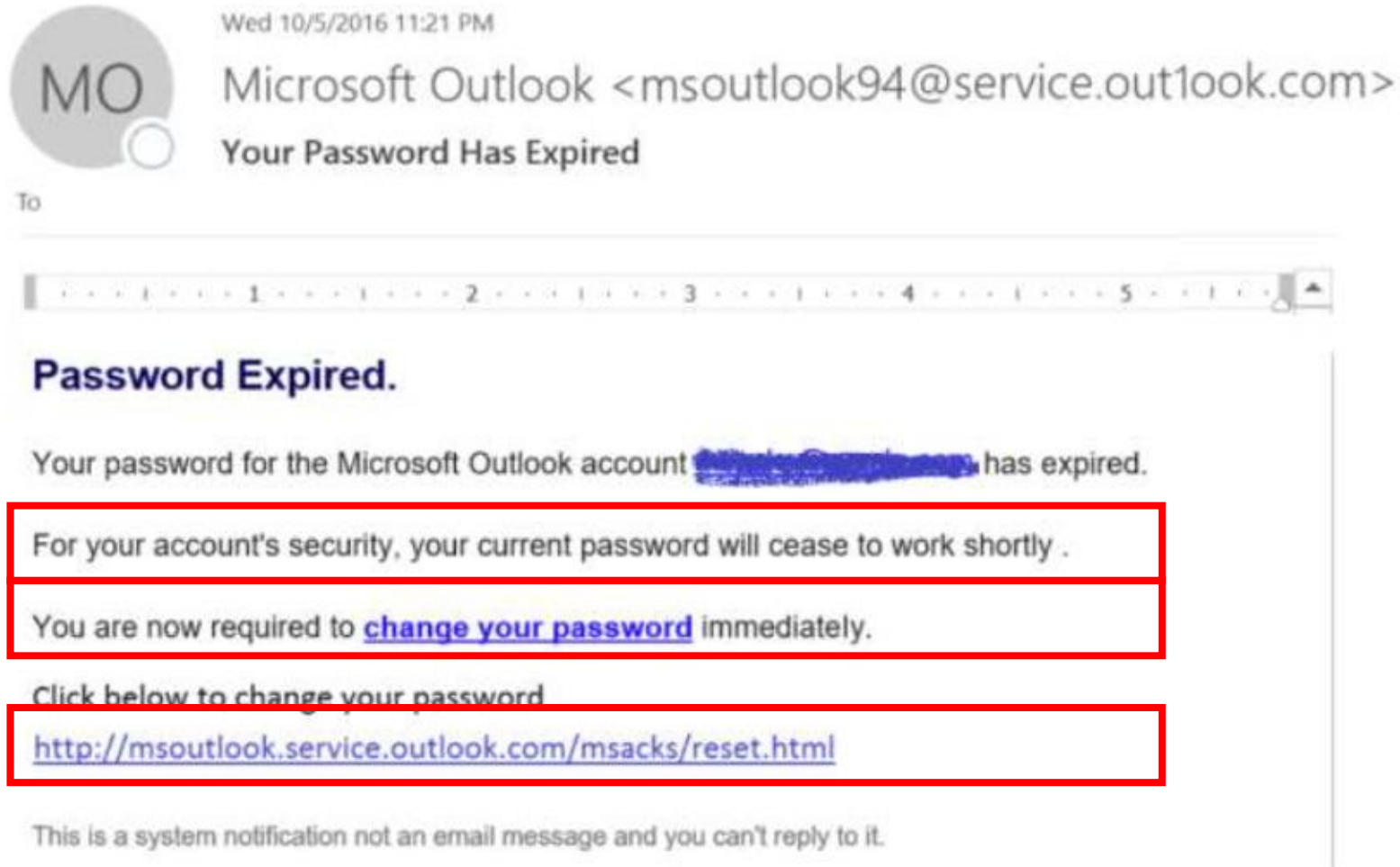
- Includes PayPal logo and chunk of fine print at the bottom
- Enforces panic

Email Account Upgrade Scam



- Relies on fear and urgency
- Account will expire unless immediate action is taken

Password Expired Scam



Encourages users to click link to update their password

Credentials are sent straight to the cyber criminal

Google Docs Scam



todder [redacted]

to: "hhhhhhhhhhhhhhhhhh@mailinator.com" <hhhhhhhhhhhhhhhhhh@mailinator.com>

bcc: "kellex@droid-life.com" <kellex@droid-life.com>

Todd [redacted] has invited you to view the following document:

Open in Docs

- Click on the link to view a document
- Reverts to an almost identical version of Gmail's login page
- Once account is selected, you are invited to grant access to your Google account
- Often appears to be someone you know

Smishing (Text Phishing)

85% of mobile phishing attacks happen through Smishing

What should we look for?

What looks suspicious in this text thread?

8:57
Amazon Alexa

62

655-265-5555

talk on the phone but let me know if you get my text

Thanks Pravin Dugel.

I have an urgent task for you, are you free ?

Yes I am just studying the Iveric Bio modules

What is it

Recognize Number?

Full Name?

Urgency

The Ask

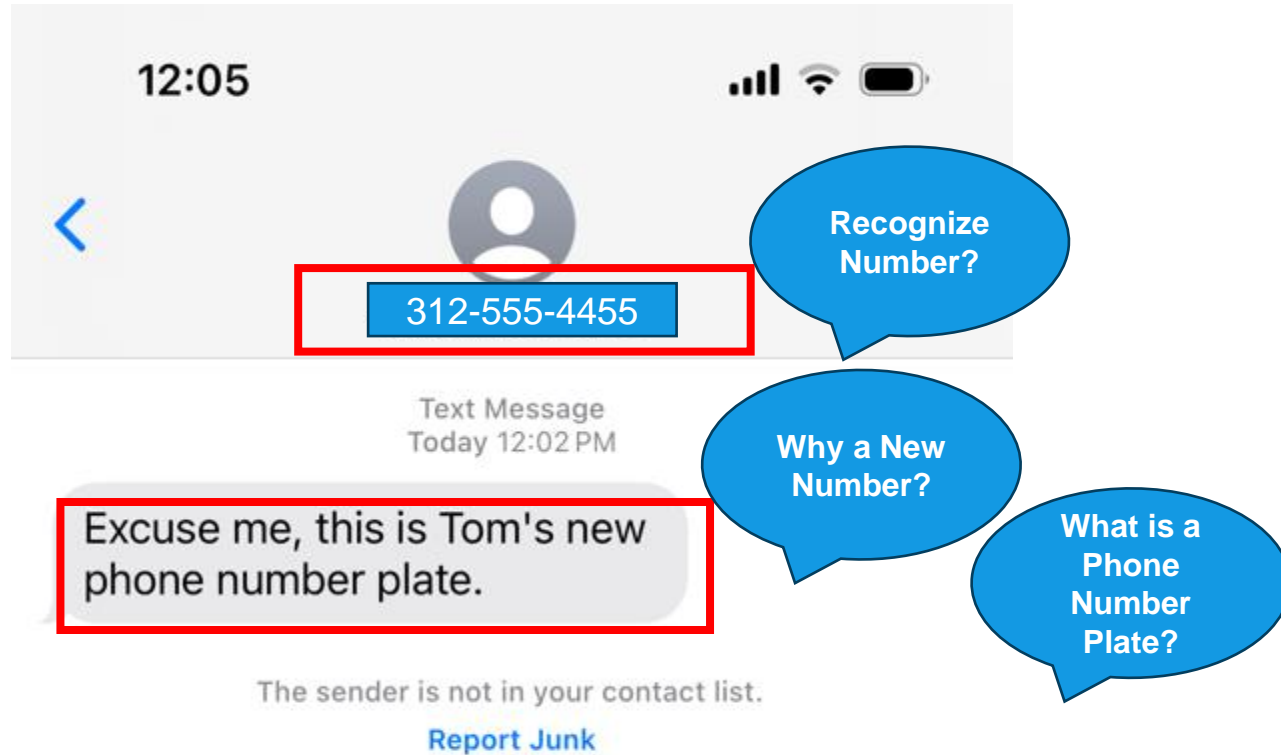
I'm on a conference call meeting right now and I need to provide a client with some cards. Can you confirm if you can purchase Apple Card's from the nearest store to you ?

No I am sorry.

Text Message

Camera, App Store, Cash, Search, Photos, Music, etc.

Phishing Texts



What do you see that is suspicious about this text?

What should you do?

1. Delete the text message
2. Block the number



Question Everything! Prevent Technology Scams

- Take a close look at the email addresses and business information on emails
- Look for spelling or grammatical errors
- Do you know this person well enough for them to ask you this?
- Is this a number you have saved for them?
- Can you call the person or text them on a new thread and confirm?
- Is there someone else who could confirm this for you?

Social Media

Social Media

Social Media is part of our everyday life.

It brings many positives, but there are also some dangers lurking out there.

Remember that not everyone has your best interests in mind!

There are ways to stay safe and be aware when using social media





Posting Pictures

- Stop and Think before posting pictures
- Do not reveal personal information like your address, car information, or current location
- Do not post pictures while still on vacation or away from home
- Look in the background of photos – are you giving away important information like your address? Or showing other people?
- Deactivate geotagging from your photos

Preventing Social Media Scams

- 1 Don't Overshare! Never fill out questionnaires that ask questions like "your favorite teacher" or "the street you grew up on".
- 2 Only accept friend requests from people you know
- 3 Clean up your friends list!
- 4 Do not geotag photos - especially when you are on vacation or away from home!
- 5 Do not post your birthday or full birthday with year anywhere
- 6 Check your privacy settings

Social Media

What goes online, stays online.

Even on apps where photos, chats, etc. disappear, people can take screen shots

Think about what you are posting! What if any of the below people came across your post. How would you feel?

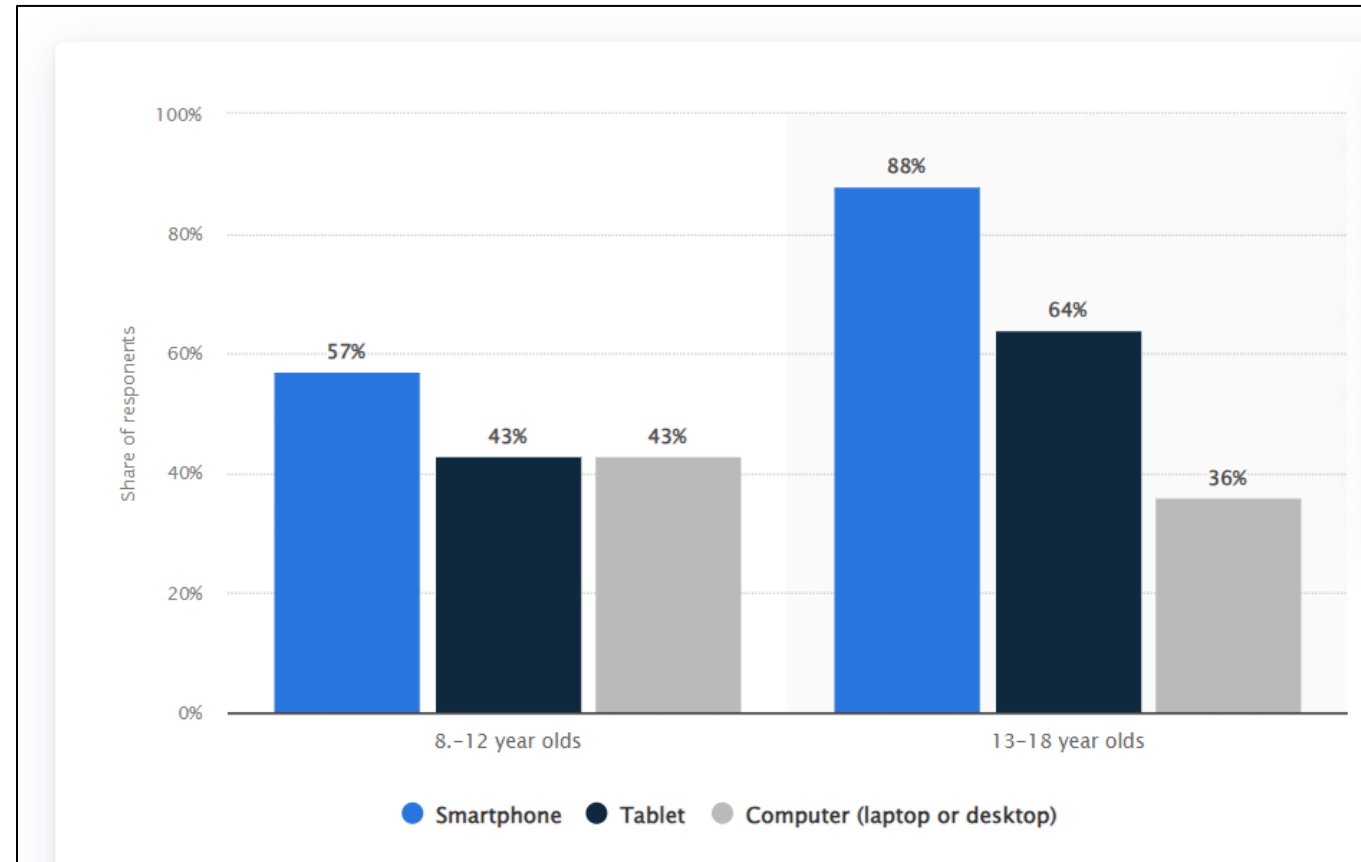
- Parents, grandparents or other family members
- Teachers, coaches
- Future employers
- Future college admissions
- Friends

If you would not want them to see it, do not post it



Protecting our Families

Share of Children with a Personal Device in the US in 2021



San Diego County District Attorney Statistics

- Fastest growing crime in the US is Internet crime; Children are the fastest growing victim pool
- Over 45M children ages 10-17 use the Internet
 - 20% have been sexually solicited
 - 25% have encountered pornography
 - Over 75% of these encounters are not reported to parents or police
 - 60% received email/message from a stranger and responded
- Parental Supervision
 - 20% do not supervise their children's Internet use
 - 52% moderately supervise their use
 - 71% stop supervising their use after age 14
 - 62% of teens say their parents know little or nothing about the websites they visit

Protecting our families

Our kids can often scroll before they can crawl. There are a few things you can do to help them stay safe:

- Educate yourself and your children about dangers
- Start safety training at a young age about downloading, cyberbullying, identity theft and more
- Cyber safety skills should become routine, like looking both ways before crossing the street



Protecting Our Families

- Agree together on rules; Monitor and regulate usage times—***especially at night***
 - Family Contract:
<https://www.sdcca.org/content/preventing/protecting-children-online/family-contract.pdf>
- Try to avoid usage in private; Spend time with them online
- If there must be a computer in a bedroom, make sure the screen faces the door
- Keep devices in a central location
- Set up central charging stations to keep all devices together



Protecting Our Families

Many devices come with easy parental controls... ***USE THEM.***

- Put accounts in your name and know your child's passwords
- Many devices can be set up so a child's account cannot be used to download or install apps without parental consent
- Routers can limit the hours of use by MAC address (address of your device)
- You can block whole website categories
- Always set up device controls before giving it to your child
- Downloading games from app stores should be restricted until the child is old enough to make this decision

Social Media

For Parents!!!

Social media is designed to keep people engaged. It learns what you like, what you look at, and how you spend your time on its platform.

Bad actors can use this information to act like they know someone.

It suggests content that supports what it has learned. It does not care how this affects your child's mental health or world views!

Your child may think he is talking to someone his age, but he is really talking to this guy! ==→

Your child should never meet someone in person that he met online!

Stay informed about who your child is talking to

Advise your child to tell you if he thinks he is talking to someone who might not be trustworthy



Protecting our Families: Chatrooms

Talk to your children about chatrooms. They can introduce your child to offensive language, sexual content and predators

Chatrooms are usually embedded within games or social media but can also be stand alone

- Many chatrooms also have webcam features
- Children—especially older children—are drawn to the anonymity
- “Stranger Danger” also applies to chatrooms



Home Safety

Home Safety

Back up your data!

- Use an external portable storage device or cloud services
- Backup your data daily or weekly
- Use the 3-2-1 rule!
 - 3 copies of your data on at least 2 different media, and 1 copy off-site
- Periodically check or verify that your data can be restored



Home Safety

Many of our homes are equipped with smart devices (Estimate 75B+ by 2025)

From thermostats to refrigerators, our homes can connect to the internet and to each other (Internet of Things or IoT)

Includes Amazon and Google Assistants – Yes! They are listening!

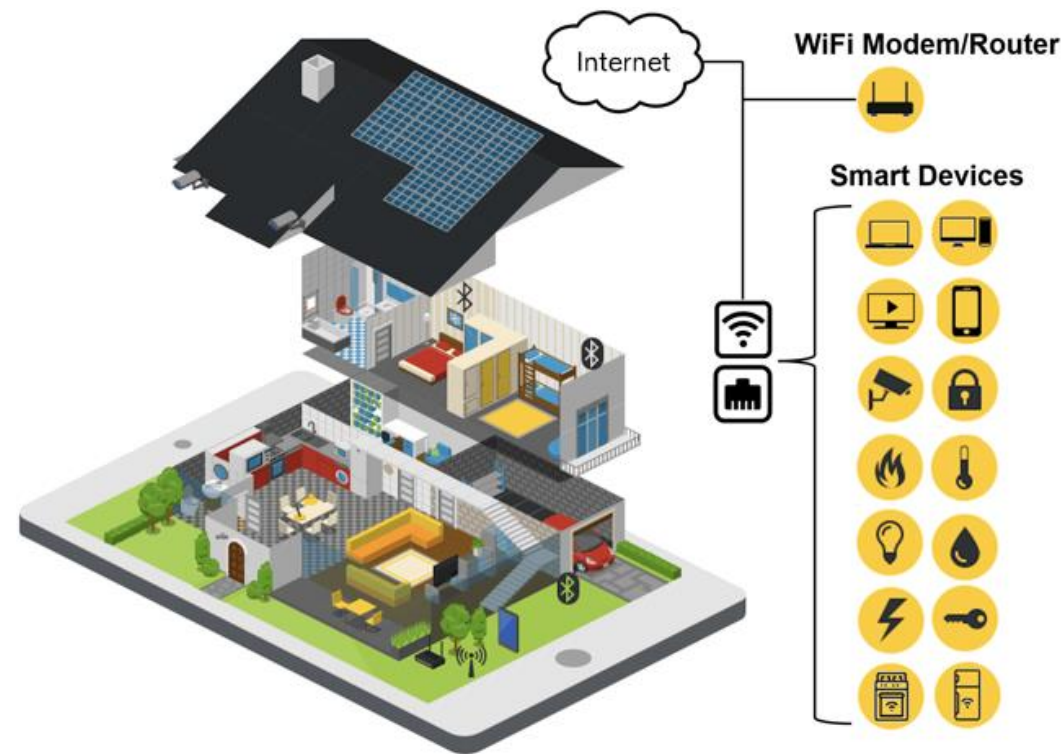
Risks

- Lack basic security features
- Default passwords aren't changed
- Software/Firmware lack security updates
- Encryption not implemented
- Devices collect and transmit sensitive data that can be intercepted
- Criminals can track usage patterns
- Phone applications to control the devices can be hacked or stolen
- Assistants can be an entry point to your home network



Home Safety

- Be careful who you give access to
 - Car remote starter, thermostats, etc. can be used by bad actors.
- Disguise your home router to protect internet surfing and browsing
 - Change the default name and password
- Set up a Guest Network for your guests to use temporarily
- Place your IoT devices on a separate network
- Implement security features for Digital Assistants (passwords, router settings, etc.)



Summary

RECAP: TOP TIPS

1. Create long, strong, unique passwords for every site
2. Be careful on public Wi-Fi connections
3. Use available tools such as Firewalls and VPNs
4. Verify website security before use; Download and stream from proper sites only
5. Question what you see in e-mails and pop-ups
6. Think before you click; Anyone asking for payments in the form of gift cards or wire transfers is most likely a scam.
7. Do not post sensitive information on social media sites
8. Protect your family with education and diligent monitoring
9. Get anti-virus protection and keep it updated
10. Keep your computer software and device apps updated
11. Back-up your pictures and documents
12. Manage your IoT devices
13. If possible, freeze your credit with TransUnion, Equifax and Experian. Most banks will assist you if you call for help
14. <https://www.pcmag.com/explainers/ramp-up-your-cybersecurity-with-pcmags-online-safety-checklist>

You Have Been Scammed, Now What?

1. Remember that you are not alone! 56% of those impacted do not know what to do next.
2. Collect your thoughts and remain calm
3. Change your passwords
4. Make a list of all information that was stolen
5. Track all communications
6. Obtain a copy of your credit report and review it
7. Notify credit card companies and financial institutions
8. Contact your local law enforcement
9. Report it to the FBI
at <https://www.ic3.gov/> and at <https://fightcybercrime.org/>



Additional Resources

Freezing Your Credit:

<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>

Antivirus Software Recommendations:

<https://www.consumerreports.org/cro/antivirus-software.htm>

Cybersecurity & Infrastructure Security Agency:

[Cybersecurity Tips](#)

Free Credit Reports :

www.annualcreditreports.com

Check To See If Your Email Account Was Hacked:

haveibeenpwned.com

Places To Check For Scams:

www.consumer.ftc.gov/features/scam-alerts

Top Tips for Parents on Cybersecurity:

http://mw.k12.ny.us/wp-content/uploads/2015/05/Safe_Secure_Parents_Top-Tips_acc.pdf

Thank You!

Cara Camping CISSP, CEH, PMP



CENTER[™]
for Cyber Safety
& Education

© 2023 ISC2. All rights reserved. Some images in this presentation are subject to copyright protection and used under license from third parties. Do not use images from this presentation without first consulting the ISC2 brand team.

What is AI?

Artificial intelligence is a machine's ability to perform the cognitive functions we usually associate with human minds

AI is a big term encompassing different types of learning like machine (algorithms and predictions) and deep (recognizing patterns or images)

AI has many practical applications in life and in the business world

It also has the potential to be used by bad actors

Where do we find AI?

- Chatbots on website
- ChatGPT
- Siri and Alexa
- Marketing and sales offices
- Spotify, Netflix, and other services that give you suggestions

Identity Theft

Identity Theft: What is it?

A “bad actor” gains access to enough information about you to:

- Open accounts in your name including credit cards and loans
- File taxes
- Make purchases
- Make claims on your insurance, medicare, etc.

This can have a lasting effect on your credit and can leave you with outstanding debt that is not yours



Identify Theft: You Are a Victim

How can you know if you have been a victim?

- You receive a lot of physical mail or email related to loans that you didn't apply for
- Credit card pre-approval or cards are being rejected under your name, regardless of if you applied for them or not
- You receive notices about your auto-pay bills bouncing
- You get a letter from the IRS about an income tax return that has been submitted
- You get notices from your insurance provider about procedures, visits, etc. that were not yours



Identity Theft: Prevent it

What can you do to prevent it?

- Use a password manager
- Be careful sending sensitive information – make sure it is a secure site
- Never use email to send your social security number or other information
- Configure multi-factor authentication (MFA) for all social media, email, financial and online shopping sites
- Do not give your information over the phone. If someone calls looking for information, hang up, look up their company number yourself, and call from that number, not the one they gave you.
- Put a credit freeze on your accounts. This can be done at all three credit bureaus – TransUnion, Equifax, and Experian.



Identity Theft: Protect Yourself

How can you protect yourself and your credit report?

- Shred all documents with personal info that you no longer need
- At least annually, check credit reports from the three credit bureaus
 - You can find them at <https://www.annualcreditreport.com/index.action>
- Place a fraud alert on your credit files or freeze your credit reports, **including your children's!**
- Review your credit card statements monthly or set alerts for all transactions
- File taxes early, before scammers can
- If you are asked to give your Social Security Number on a form, ask if they really need it
- If you are impacted by a breach and are offered free credit monitoring services, use it



Identity Theft: Next Steps

What do you do if it happens to you?

1. Stay calm – you are not the only one
2. Place a fraud alert on your credit report
3. Contact your bank and any other companies where the theft is occurring. Close out accounts that have been tampered with or opened fraudulently.
4. Report the identity theft to the Federal Trade Commission at <https://www.identitytheft.gov/#/>
5. File a report with your local police department