

Staying safe on the Internet

YMCA/Fifty Forward
January 2024

Jaqui Lynch
Circle4 Consulting
jaqui@circle4.com
<http://www.circle4.com/papers/safetypres.pdf>



Agenda

- Terminology
- In person and using Contractors
- Travel Safety
- Risks and Computers
- Email
- Chat, IM, Texting and Social Media
- Online Shopping
- Cyber Stalking
- Firewalls and Antivirus
- Examples
- Tips
- Questions



Terminology

- <https://www.fcc.gov/scam-glossary>
- Robocall
- Catfishing
 - Catfishers create fake identities on dating apps and social media to coax you into fake online relationships. They often quickly move to personal channels such as phone or email, using your trust to acquire money or personal info, or help you hide their criminal activities.
- Identity Theft
- Phishing and Social Engineering
- Smishing is SMS Text Phishing
 - Often involves text messages claiming to be from your bank or another company. The message displays a phone number to call or a link to click, giving scammers the chance to trick you out of money or personal information.
- Doxing
 - The collection and publication of an individuals' personal information for malicious intent. You'll probably never meet them in person. A form of cyber harassment
- Many many more

Popular Scams

- Disconnection threats – power and gas
 - Through email, scammers will target customers by using a utility company's official logo and prompting customers to use Bitcoin to make payments through a QR code. Gas and electric never use bitcoin
- Utility work imposters
 - Always insist on seeing ID. If unsure call the company and ask if this is legitimate
- Impersonation Scams
 - The scammer reaches out to you pretending to be someone you trust to get sensitive information like social security numbers, bank information, or Amazon account details. May pretend to be relative desperately needing money.
 - Be wary of false urgency.
- Gift Card scams
 - Gift cards are the most common way scammers seek payment from their targets, according to Federal Trade Commission. Con artists use Target, Walmart, iTunes and other popular gift cards as cash conduits in impostor and phone scams. The nearly 65,000 consumers who filed complaints with the FTC about gift card payment scams in 2022 lost a total of \$228.3 million. They may claim to be from IRS or many other places.
- Delivery scams and cons

Medicare Scams

- 1. COVID fraud
 - Criminals offer free coronavirus tests as a way to gather people's Medicare numbers and other personal information and file fake claims in their name.
- 2. Bills for diabetes supplies
 - Claims for continuous glucose monitoring devices are showing up on Medicare summary notices for people who don't have diabetes and didn't receive the device, she says. The scammers charge Medicare.
- 3. Flimsy medical equipment
 - Con artists offer you a knee brace or other medical equipment if you give them your Medicare number. You'll get a cheap brace in the mail that you could have purchased at a drugstore, or you might receive no brace at all. The criminals charge Medicare for an expensive brace and make other unauthorized charges with your number.
- 4. Bogus genetic testing
 - Even though the Senior Medicare Patrol helped uncover a \$2.1 billion genetic testing scam, phony pitches are still an issue. Someone at a health fair might offer to swab your cheek and test the sample to determine whether you have a genetic propensity for cancer. You need to give your Medicare number to cover the test, the con artist says.
 - In reality, Medicare rarely covers genetic testing. Scammers use the ploy to get your Medicare number and make all sorts of fraudulent charges in your name.

Medicare Scams

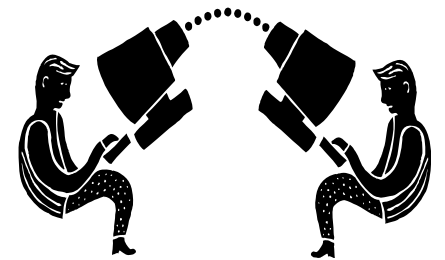
- 5. Hospice fraud
 - scammers enroll people who aren't terminally ill in hospice without their knowledge. The Medicare beneficiaries instead may believe they are signing up for extra benefits programs, such as home cleaning, in-home nurse visits or a shower chair.
 - They have a doctor that works with them and is 'diagnosing people' and sending paperwork to Medicare and claiming thousands of dollars that Medicare pays for in hospice.
 - The criminals receive payment from Medicare for hospice services never delivered. The Medicare beneficiary has legitimate nonhospice claims denied.
- 6. Medicaid 'unwinding'
 - During the COVID public health emergency, beneficiaries of Medicaid, the federal-state health insurance for low-income Americans, didn't need to recertify eligibility based on their income. When the emergency ended in May, states began to ask Medicaid recipients for recertification. Scammers began calling Medicaid beneficiaries and telling them they need to pay them, so they don't lose Medicaid. They are also using it to get beneficiaries personal information."
- 7. Next generation Medicare cards
 - Medicare saw a big increase in card scams in 2018 when the government sent every beneficiary new cards that didn't include Social Security numbers. Senior Medicare Patrol volunteers are seeing some card scams resurfacing. The scammers ask for money for the new card or ask for your Medicare number. Medicare won't call you to offer a new card, its cards are paper stock and you can print an official card from your online Medicare account anytime. What's more, Medicare won't ever call you without scheduling an appointment ahead of time.
- 8. Telemedicine sessions
 - You may get a call from somebody who is trying to sell you something, and then you'll get billed for a telehealth consult

Skimming Scams

- Skimming scams are targeted at people using ATMs, gas pumps, or credit card readers at retail outlets. The scammers carefully craft devices that look like legitimate card readers, which they then attempt to “blend right in” to the actual machine. Once a victim swipes their credit card, the skimming device either stores or sends the victim’s information, for the criminals to retrieve.
- Scammers have also been known to use hidden cameras to record victims entering their PIN numbers into ATM machines, the FBI said. Some also create fake numerical keypads that record the keystrokes of users, to steal such passwords.
- Be sure to inspect the reader and look for any loose parts or damage. Scratches or damage to adhesive tape can also be indicators that it has been tampered with. If you give the skimmer a light shake and it feels loose, tell an employee.
- To prevent cameras from capturing your passwords, the FBI recommends users cover the keypad with one hand, while punching in the PIN with the other.
- <https://www.newsnationnow.com/us-news/recalls/credit-card-skimming-scams/>
- <https://consumer.ftc.gov/consumer-alerts/2018/08/watch-out-card-skimming-gas-pump>

Privacy

- Know how information is being shared
 - Registration information for products such as MS Word
 - Opt out versus opt in
 - Win ME – control panel – automatic updates
 - Realplayer
 - Winamp
 - Media Player
 - Napster
 - 3D Frog Frenzy and many more
- Have a gmail or other email address just for registrations, etc
- Even if filling in forms in person – ask how they use your information and if they share it



In Person and Contractors



In Person

- Check out contractors
 - Google search them
 - www.bbb.org
 - Also your neighborhood such as nextdoor or friends
 - Ask for references
- Check their licenses at
 - <https://search.cloud.commerce.tn.gov/>
- Never let them take anything away to work on without a receipt
- Always get written quotes
- Never let them know you live alone
- Arrange to have someone else present while they are there if possible

Places to Check

www.bbb.org

Roofing Contractors, Painting Contractors, Home Improve

BBB Rating: A+



Customer Reviews



Average of 7 Customer Reviews

[Read Reviews](#)

[Start a Review](#)

Customer Complaints

This business has 0 complaints

[File a Complaint](#)

<https://search.cloud.commerce.tn.gov/>

License Details

Home Improvement Contractors

Home Improvement Contractor

1358

Active

08/31/2024

Online Dating

- <https://www.rainn.org/articles/online-dating-and-dating-app-safety-tips>
- Use different photos for your dating profile than you have anywhere else on social media or online
- Avoid connecting with suspicious profiles
 - No bio, no linked social media, only one picture
- Check out potential date on social media
- Block and report suspicious users
- Wait to share personal information
- Don't respond to requests for financial help
- <https://consumer.ftc.gov/articles/what-know-about-romance-scams>

Online Dating - Meeting

- Video chat first
 - This can be a good way to help ensure your match is who they claim to be in their profile. If they strongly resist a video call, that could be a sign of suspicious activity.
- Tell a friend where you are going
 - Take a screenshot of your date's profile and send it to a friend. Let at least one friend know where and when you plan to go on your date. Text on arrival and departure.
- Meet in a public place
 - Avoid meeting in public parks and other isolated locations for first dates.
- Don't allow them to pick you up or take you home
 - Avoid getting into a vehicle with someone you don't know and trust, especially if it's the first meeting.
- Watch any drinks that are poured for you
- If uncomfortable when you meet them enlist the help of the bartender or waiter
- **Trust your instincts**

Travel Safety



Travel Safety

- Register with your embassy if going overseas
- Check the state department for warnings
 - <https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html>
- Get travel insurance
 - There are many options - I like <https://www.allianztravelinsurance.com/>
 - For major international I also get repatriation insurance – one example is <https://www.globalrescue.com>
 - Check what your credit card includes for travel and/or rental car coverage
- Share your itinerary with someone and check in regularly – have a plan of action if they don't hear from you
- Notify your bank so they don't freeze your credit card
- Write down emergency information – local and wherever you are going
- Book travel with trusted sources to avoid being scammed
- Don't dress so you look like a good target – fit in!
 - No expensive jewellery, etc
 - Dress appropriately for the culture (cover shoulders and no shorts in churches, etc), avoid logos

Travel Safety

- Bring a small first aid kit for minor injuries
- Use a VPN when in hotels or on wifi
- Study maps before venturing out – don't stand around looking lost
- Watch for pickpockets – avoid crowded areas
- Have copies of your documents in your carry on
 - Leave a copy with someone
- Have a decoy wallet
- Check with concierge on which taxis are safe to use and discuss the price before you or your bags get in the car
- Lock all your bags at all times
- Get a cut proof purse (travelon is an example) that can also be locked
- Travel in groups
- Don't look like a victim - Be aware of your surroundings
- Check your room and closet etc, count doors to fire exit and make sure the exit is clear
- Hotel Prepay scam – don't give credit card info to people who call you
- Check bed for bedbugs before opening bags. Never leave bag open and never put it on the bed

Risks and Computers



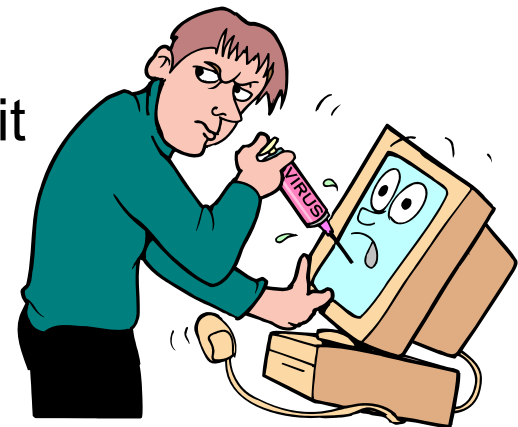
Risks

- Exposure to inappropriate material - porn, gory sites
- Physical molestation
- Harassment
- Legal, Financial, Scams & Frauds
- Privacy
- Identity Theft
- Drugs, alcohol, tobacco, bombs and other
- Gambling
- Children are naive – for a free gift they will provide any information asked for
- Inappropriate behavior – sending threats as a joke and so on
- Viruses, cookies, security holes
- Attachments with malware in them

Computers













- Windows

- Keep it patched
 - Ensure you are on the latest Windows and it is up-to-date!
 - windowsupdate.microsoft.com
 - I check weekly
- Run Antivirus and keep it up to date
- Get a bidirectional software firewall
- Backups!!!!
- Turn on ransomware protection if your antivirus offers it
- Upgrade software apps to latest versions
- Turn off file sharing unless you know how to secure it
- Try an alternate browser – 75% target IE & Edge
 - Firefox or safari or some other
 - Patch your browsers (go to help and about)

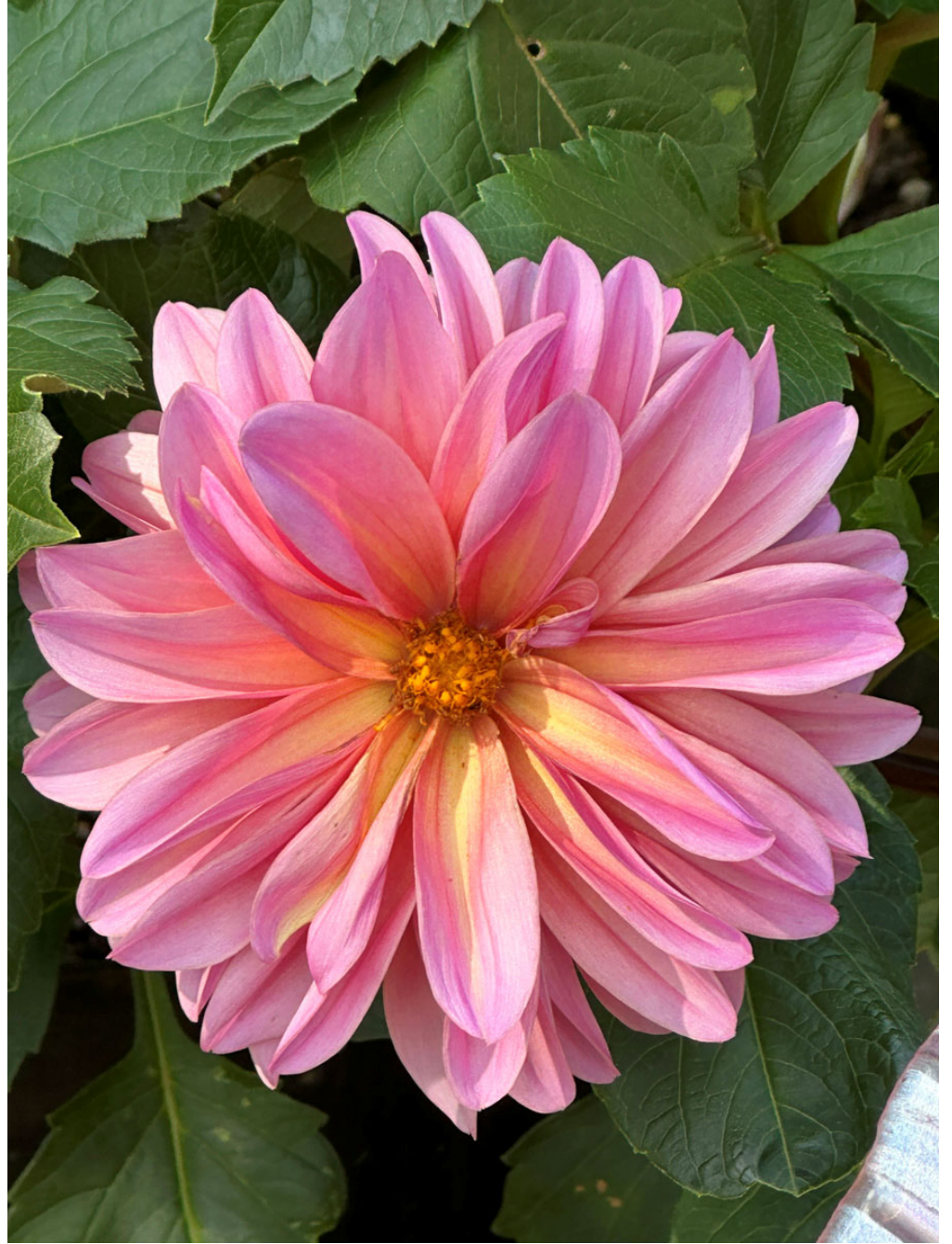


AARP Frauds and Scams Site

- Lets you search on scams reported in your area
- <https://www.aarp.org/money/scams-fraud/>
- Great article on 7 Tips to Stop Porch Pirates

Date occurred ▼	Scam type	Contact method	Zip code	Amount lost	Details
Dec 23, 2023	Cryptocurrency Scams And Fraud	Advertisement	37217	\$1001-5000	VIEW DETAILS 
Investment in fake web site			 	Learn more about undefined scams > Signup for the latest scam alerts >	
Nov 15, 2023	Online Relationship Scam	Other	37062	\$1001-5000	VIEW DETAILS 
Met on BBW (bustr) date site. He claimed to be a tailor designer for Ralph Lauren. Of course he proclaimed his love right away. I loaned him money. Then he made like he wrongly sent me money by WISE and forgot to pay the fees. As me to loan him some money. I'm out \$4000 for feed to WISE HE said. Not so. On and on it went. I was stupid. Sending him money			 	Learn more about undefined scams > Signup for the latest scam alerts >	
Nov 8, 2023	Tech Support	Internet/Email	37069	\$1-100	VIEW DETAILS 
Microsoft notification popped up on my screen said computer had been locked to call Microsoft at 1-833-493-3303 for help. Said a number of things on screen i.e., do not turn off computer, etc.			 	Learn more about undefined scams > Signup for the latest scam alerts >	
Oct 31, 2023	Government Impostor Scam	Internet/Email	37211	\$101-500	VIEW DETAILS 
passport scam took 214.00 from me			 	Learn more about undefined scams > Signup for the latest scam alerts >	

Email



Email



- Treat it like a postcard
- One to one communications
- Spam
 - Never reply as you confirm your address
- Use inbox protection (hotmail) or filtering and/or blocking
- Never say anything that you wouldn't say in public
- Remember ISPs back this stuff up
- No visual or audio cues so people take it literally
- **NEVER** open attachments in an email or text or click on links without checking with the sender first that they really did send them no matter who it is from!!
 - Even then download the attachment and scan it first with your antivirus software

Email Abuse

- Spam
- Scams
- Phishing
- Flaming
- Harrassment and stalking
- Spoofing
- Mail bombs
- Viruses
- Chain letters
- Pornography
- Photos
- Inline html and/or pdfs



Chat, IM, Texting and Social Media



Chat rooms & Social Media

- Let you talk to groups of people all around the world
- Public or private groups
- Most dangerous area of the net
 - You don't know who is there (actively or lurking)
 - You establish a relationship and trust over time
 - Pedophiles use them to find victims
 - People lie
- They often progress to IM and email where you are now one on one
- Choose a vendor neutral screen name
- Turn on logging
- Be careful what you say
 - People can log it and build up a profile over time
- If you end up in a flame war or being attacked walk away and stay out of the chat for a while

Social Networking sites

- **Public forums:**
 - <http://www.facebook.com>
 - Linked In
 - Youtube
 - Twitter – now X
- **Thing to remember**
 - What you put up stays around (caching)
 - It is publically accessible and will be forwarded
 - Employers and universities search these sites
 - What do you want your online identity to be?
 - With freedom comes responsibility
 - Respect both your own and others privacy
 - Same rules apply in virtual worlds
 - Second life
 - Runescape
 - Minecraft, etc
 - Make sure someone monitors your kids/grandkids on these sites

Instant Messaging & Texting

- Unique identifier associated with profile
- Real time – more IM than email
- Blend of email and chat
- ICQ was the forefather to IM
- Runs in background and notifies you when there is a message
- Buddy list – a notify list of friends
- Skype and Video conferences/cameras



The Dark Side of IM

- Protect your buddy/contacts list - set it so you have to approve the addition of anyone to it
- People can add you to their buddy list and then keep track of when you are online
- Set your options so others can't add you to their buddy list
- Predators love buddy lists
- They also love being able to search profiles and membership directories
- Don't let anyone who is not on your contact list text you

Profiles & Directories

- At most sites you can search the directory by:
 - Keyword
 - Gender
 - Age
 - Interests
- Requesting profiles with pictures
- Asking whether they are online now
- Regularly use Google or similar to search on yourself
- Never fill these out truthfully
 - When I sign up for an online game I lie about my age, gender, state etc
- Predators use these to determine victims
- NEVER put personally identifying information that could be used to target you
 - i.e. you age and gender and address and that you live alone

Phone Calls

- If you don't recognize it let them leave a message
- Never answer yes – they can then record you and use it later
- If they say “is this Jaqui” the correct answer is “who am I speaking with?”
- Never give a person on the phone a code that is texted to your phone – they will never call and ask for it
- Don't call back on numbers they give you – use the one on your card
- Don't give personal information to anyone that calls you – credit card numbers, social security numbers etc etc
- Watch for jury duty, IRS and other scams that ask you to pay in gift cards or to call back
 - If you are worried, then find the department on the web and call the published number
- Watch for Microsoft and apple etc support calls – they are not real

Telephone and Text Scams

- You get an email stating you need to call a number or they will take legal action regarding a debt
- Don't call – a credit agency should send a letter
- If you call you will probably find it is not a toll free number and your next bill you will have a \$25 per minute charge on it
- Suspect area codes:
 - 758, 787, 869, 876
 - 441, 242, 246, 268
 - 345, 809
 - And many many more

Online Shopping



Online Shopping



- Be as careful as you would be in a store
- Make sure it is https, not http
- Look for https and the lock at the bottom right
- Hover over a URL in an email and make sure it really is the site you think it is supposed to be
- NEVER put your credit card into a site that uses ip numbers in the URL

- Print a copy of the online order
- Use only one card for all online purchases
- Check out new companies with the Better Business Bureau
- If an offer looks too good to be true then guess what



Common Sense

- Have one credit card that you use online
- Check that card statement regularly
- Never give your credit card number to someone who calls you
- Never post where you are especially when on vacation. Post pictures when you are back
- Don't engage – don't try to play games with them
- No-one legitimate will ask you for your username and pin by phone or email
- Teach your kids and others never to download things
 - I.e. don't accept gifts from strangers

Cyber Stalking



Cyberstalking – what is it

- Can be harrassing or threatening emails
- Postings to news or lists or on the web about you
- Mass unsolicited email – a favorite is to subscribe you to listservs against your political/religious beliefs
- It does happen even to people who never go online
- Identity theft
- Mail spoofed as if you sent it
- Viruses sent to you
- Hacking attempts
- You name it – they'll try it
- It can escalate to offline encounters

Cyberstalking – what to do

- Don't respond to flames
- Don't flirt online – it escalates very quickly
- It does happen even to people who never go online
- From www.ccmmostwanted.com
 - Use a PO Box for mailing – even on your checks
 - Use an unlisted and unpublished telephone number
 - Use encrypted email
 - Change your password regularly and don't write it down
 - Change your username immediately
 - Use an ambiguous username
 - Save all messages and record dates and times
 - Contact one of the agencies such as National Victims Center, Cyberangels, WHOA and get advice and help

Firewalls, Antivirus



Personal Firewalls and Antivirus

- Do a search on the web for “personal firewall”
- Critical if you are using DSL or Cable Networking especially if you use public wifi
- Bitdefender
 - <https://www.bitdefender.com/>
- Zone Alarm
 - <https://www.zonealarm.com/>
- Norton 360
 - <https://us.norton.com/products/norton-360-standard>
- McAfee Personal Firewall
 - www.mcafee.com
- Backup your data and email regularly
- Run antivirus
 - If it offers anti ransomware turn that on



Scan yourself

- Run a scan
- https://www.trendmicro.com/en_us/forHome/products/housecall.html
- Norton Power eraser
 - <https://support.norton.com/sp/static/external/tools/npe.html>
- Many others

Tips



TIPS from fraud.org

- Know who you are dealing with
- Only call the number on the company's website or your membership card
- Have a safe way to pay
 - Paypal, venmo, one dedicated credit card, etc
- Guard your personal information
- Don't send sensitive information such as credit card numbers by email
- Use https for websites that you are making payments through
- Do not trust unsolicited emails or texts
- If it looks too good to be true – IT IS
 - There is no such thing as easy or free money
- Get off credit marketing lists especially ones that send offers in the mail
- SHRED anything personal – do not throw in the trash
- Check your credit cards and bank accounts regularly
- Make sure you understand anything you sign or agree to
- Request your annual credit report
 - <https://www.annualcreditreport.com/index.action>

Tips to staying safe



- Keep your identity private
 - Never give out name, address, phone
 - Don't mention your city or school & never provide photos
 - Lie in your online profile
 - Use a gender neutral screen name
 - Don't reveal anything about your friends either
- Never get together with someone you meet online
 - Online dating – meet in a public place and take a friend
- Never respond to email, chat, messages that are hostile, inappropriate or make you feel uncomfortable
- Never give out your password and don't let others post from your account/computer **EVER**
- Be extremely careful with video cameras

Tips to staying safe

- Don't list yourself in the members directory at your ISP or gmail, yahoo, ICQ, IM
- Keep an eye on your IM buddy list and contacts – secure it
- Be careful what you put in the registration files for things like Office – they get embedded in any documents
- If email needs to be confidential use PGP and encrypt it or don't send it
- Regularly search on yourself at the social networking sites and on google
- If putting up pictures use small ones that are a little fuzzy
- Never put children's photos up without password protection

- NEVER open attachments until you check that the sender really did send them
- Don't proliferate scams, etc – check at snopes
 - <https://www.snopes.com/>



Extras

- Be careful on social networking sites
- Check how much you are revealing over time
- NEVER meet anyone in real life that you met on the internet without taking steps to protect yourself
 - Bring a friend
 - Meet in a public place
 - Have a getaway plan
- Human friends are better than computers and healthier
- If you post pictures on publically accessible sites
 - Be prepared for someone to paste your head on someone else's body or vice versa
- Don't post pictures of kids anywhere on the web
 - They will turn up in kiddy porn later
 - If you must post them do it in groups with no names or addresses
 - Make sure the school isn't putting up photos of your child with identifying information
 - Watch out for those "build an autobiographical website" projects at school and elsewhere

Parents Extras

- Have your child set up an account for you
- You should be the only one with the internet router password
- Make sure they don't turn on Parental Controls or filtering
- Understand the services
- Monitor your kids activities – no computers outside of public places
- Limit computer time
- Sign a family internet usage agreement
- Human friends are better than computers and healthier
- Don't post pictures of your kids anywhere on the web
 - They will turn up in kiddy porn later
 - If you must post them do it in groups with no names or addresses
 - Make sure the school isn't putting up photos of your child with identifying information
 - Watch out for those “build an autobiographical website” projects

TIPS 1/2

- Select a gender neutral username
- Keep your real email address private
- Get a free email account (gmail, hotmail, yahoo)
- Don't fill out profiles – if they make you put your age or sex – lie.
- Don't answer those internet polls/questions where you are supposed to tell 25 things about yourself. Same with the games that ask personal questions.
- Block, filter or ignore unwanted users
- Never defend yourself
 - You will be flamed
 - it is better to change screen identities
- Lurk on facebook or neighbourhood pages before posting or speaking

TIPS 2/2

- Watch what you say online
- Make sure you know what is in your signature file
- Get an unlisted telephone number
- Get callerid
- Search for yourself and your kids regularly at google, bing, etc
- Never share your password
- No pictures online anywhere and don't let your kids school put your kids picture up

- Set up multifactor (or 2 factor) authentication on all accounts
- Have credit card companies, airlines, etc text or email you whenever something is charged to your account

References

- <https://reportfraud.ftc.gov/#/>
- <https://www.ic3.gov/>
- Company checking
 - <https://www.bbb.org>
 - <https://search.cloud.commerce.tn.gov/>
- Fact checking
 - <https://www.snopes.com/>
 - <https://www.scambusters.org>
- www.fraud.org (National Fraud Information Ctr)
 - <https://fraud.org/prevention-tips/>
- <https://www.annualcreditreport.com/index.action>

Summary

- Teach yourself and your kids to be safe
- Remember that the Cyberworld poses the same risks as the real world – never do something on the net that you wouldn't do normally
- Common sense is worth more than banning use
- If you get stuck – ask a 12 year old for help
- Have a family agreement about internet use

Examples



Phishing email

From Remit_Advice@jpmchase.com
To Jaqui Lynch
Cc edi.distribution@jpmchase.com
Subject **JP Morgan Chase Report - 10000014331786 #secure#**

Reply Reply All Forward Archive

JPMORGAN CHASE & CO.

Remit_Advice@jpmchase.com is using Virtru to send and receive encrypted email.

Unlock Message

UNENCRYPTED INTRODUCTION

Note: Please be advised, after 90 days from the date of this email, you will no longer be able to decrypt and view this email. If necessary for your business with JPMC, please save the decrypted content of this email in a secure location for future reference.

1. I don't have a JPM Chase account
2. The domain should be chase.com

When hover over link I see:

```
https://jpmchase.secure.virtru.com/start/?  
c=experiment&t=emailtemplate2019-09&s=Remit_Advice%  
40jpmchase.com&p=e5d02743-ed73-465c-9271-519421c90ed3#v=3.0.0&d=https%3A%  
2F%2Fapi.virtru.com%2Fstorage%2Fapi%2Fpolicies%2Fe5d02743-  
ed73-465c-9271-519421c90ed3%2Fdata%2Fmetadata&dk=  
0F837gUzJABhZlFa4tV2nqMzd1rqK9LEIdFTNiAiNT0%3D
```

Airline Account Hack

- Feb 2023 got an email from airline saying:

Great news! We've successfully completed your request and are pleased to present you with the following AAdvantage® award:

Date issued	Miles redeemed	Recipient	Description
02-26-2023	50,000	DAMIAN DUNCAN	Flight award

If you did not authorize these miles to be deducted from your account, please [contact us](#).

- I had not done this so I called them at the 800 number on my membership card
- Turns out someone had broken into my account so we cancelled their trip
- To get my miles back I had to file a police report for identity theft and provide the report number back to the airline
- The police told me they don't deal with wire fraud and had me report it to IC3 – Internet Crime Complaint Center
- NOTE if I had not set my account up to email me when something happened then I would not have known till too late
- That account now has Multifactor authentication turned on so I need the user name, password and a number that they text to me

Internet Crime Center

- <https://www.ic3.gov/>

Protect one another.

The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cyber crime. It is run by the FBI, the lead federal agency for investigating cyber crime. Here on our website, you can take two vital steps to protecting cyberspace and your own online security.

First, if you believe you have fallen victim to cyber crime, file a complaint or report. Your information is invaluable to helping the FBI and its partners bring cybercriminals to justice.

Second, get educated about the latest and most harmful cyber threats and scams. By doing so, you will be better able to protect yourself, your family, and your place of work.

Anyone can become a victim of internet crime. Take action for yourself and others by reporting it. Reporting internet crimes can help bring criminals to justice and make the internet a safer place for us all.

[File a Complaint](#)

Join the fight against internet crime!

Spotting Scams

Can You Spot a Scam?

Here are three questions to consider when avoiding scammers.

- 1 Are you being pressured to act immediately?**
Imposters may try to rush a reply or payment. Pause for a moment and make sure the email, call, or SMS is legitimate.
- 2 Did someone request your personal information?**
Don't share any personal info, like your Card number, bank details, or codes via social media, SMS, email, or phone, especially if the request comes from an unknown source.
- 3 Are they asking for unusual methods of payment?**
Examples include gift cards, wire transfers, or payment apps.

Bank Tips



Pause before you act

Look out for unexpected attachments, typos and unfamiliar addresses. A message that urgently requests personal information could be an attempt to trick you, known as phishing. Don't click on suspicious links!



Activate multifactor authentication

Add another layer of security and turn on multifactor authentication to request a code via email or phone in addition to your username and password. You'll also be made aware of any unauthorized or fraudulent attempts.



Create strong passwords

Protect yourself with a unique password for each of your online accounts and avoid any common words—that means no favorite pet names, birthdays, cities or states.



Keep on patching

Enable automatic updates wherever possible to ensure your apps, browser and software stay up to date. Patches are released regularly to improve security and minimize your risk of a potential attack.



Look before you click

Don't always trust the first online search result you see. It could be a malicious webpage created to target popular search terms and collect account information, credentials or spread malware.

Noone legitimate will ask for:



Full ID
Details



One-Time
Verification
Codes



Username and
Passwords



Full Card
Details
or PIN

FTC Dirty Dozen

12 Scams most likely to arrive via Bulk Email

1. Business Opportunities
2. Bulk email trying to sell you things
3. Chain letters usually involving money
4. Work-at-home schemes
5. Health and diet scams
6. Effortless income

FTC Dirty Dozen

12 Scams most likely to arrive via Bulk Email

7. Free Goods
8. Investment Opportunities
9. Cable descrambler kits
10. Guaranteed loans or credit on easy terms
11. Credit Repair
12. Vacation prize promotions

Nigerian Scam – they offer you millions of govt money

Call 1-877-FTC-HELP to get info or file complaints

www.ftc.gov is the website