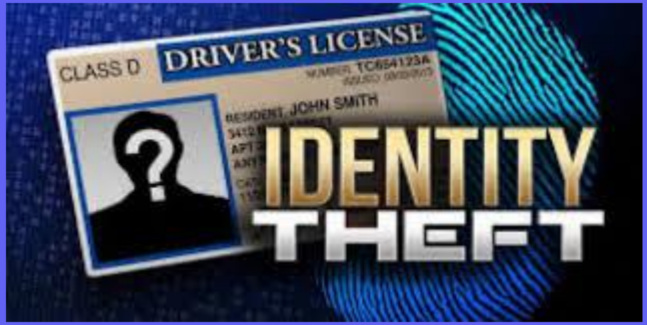


IDENTITY THEFT

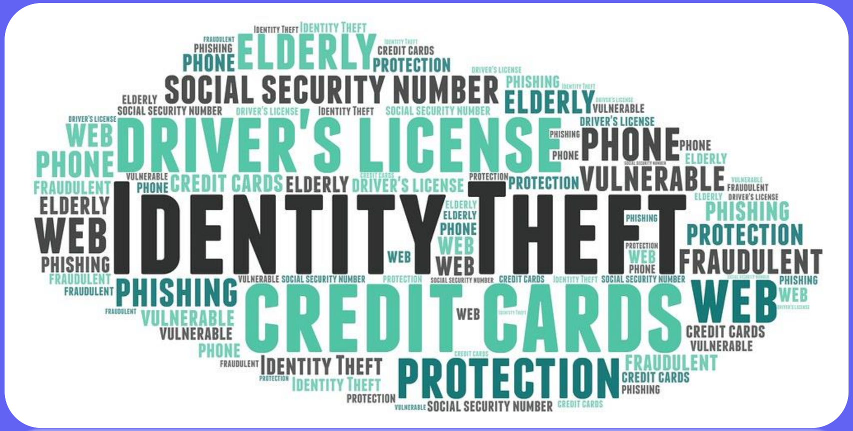
By

Bill Crowe

CONTENT

- Presentation 1
  - What Is Identity Theft?
  - What Are The Most Common Ways That Identity Theft Happens?
  - Five Common Types Of Identity Theft.
  - What Are The Current Scams?
  - What Do Criminals Do When They Have You Identity Information?
  - What Can You Do About It, If It Happens?
- Presentation 2
  - What About Malware.
  - Computer Scams.
  - Voluntarily Giving Your Identity Away.
  - Passwords
  - Email Scams
  - Conclusion.

WHAT ARE IDENTITY THEFT AND IDENTITY FRAUD?



Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

WHAT ARE THE MOST COMMON WAYS THAT IDENTITY THEFT HAPPENS

- Watch you

- Listen to you

- Email Spam

FIVE COMMON TYPES OF IDENTITY THEFT

1. Driver's license ID Theft.

2. Social Security ID Theft .

3. Medical ID Theft

4. Character &Criminal ID Theft

5. Financial ID Theft

FIVE COMMON TYPES OF IDENTITY THEFT

- The good news is:
  - Law enforcement
  - Laws have been passed to help restore your identity and credit

FIVE COMMON TYPES OF IDENTITY THEFT

- In the meantime, monitor your personal information closely.
  - Bank accounts.
  - Credit card statements.
  - Get copies of all your national credit reports at least annually.
    - Experian
    - Equifax
    - TransUnion
  - Monitor your national credit with a service like Credit Report Monitoring service.
    - Identity Guard
    - Identity Defense
    - Life Lock
  - Cross-shred all personal information.
    - credit card offers.
    - junk mail.
    - anything with your personal information on it.

WHAT DO CRIMINALS DO WHEN THEY HAVE YOU IDENTITY INFORMATION

- Mortgage Fraud
- Credit and Debit Card Fraud
- *Prize and Lottery Fraud
- Debt Collection Fraud
- *Grand Child Scam
- Jury Duty Scam
- *Computer Repair Scam
- Fake charity

PRIZE AND LOTTERY FRAUD

Fake lottery scams, many of which are foreign, exhibit well-known signs that something is wrong:

- You receive notification that you are a "winner" but need to send money to the lottery or sweepstakes office to cover taxes or administrative costs.
- Your winner notification arrives by bulk mail.
- You are required to attend a meeting to collect your prize.
- You don't remember entering the lottery or sweepstakes.
- Any payments you make are followed by more requests for cash or you are contacted by other organizations claiming you won their lottery as well.

PRIZE AND LOTTERY FRAUD

What You Can Do

There are a number of steps you can take to protect yourself:

- Never pay money to collect on a lottery or sweepstakes. Legitimate taxes can be taken out of your winnings.
- Don't share your credit card or bank account numbers or send money even if the organization sends you a check—which is probably bogus.
- If you think the prize might be real, research the name of the company or organization and contact it at a known phone number.
- Report all suspected scams to the FTC.

GRANDKID SCAM

Herald Tribune

- **Grandkid Scam:** You receive a call from an unknown person, usually pretending to be a law enforcement official or an attorney, telling you that your grandchild or other family member or friend has been arrested or otherwise detained by law enforcement and you are asked to purchase Green Dot cards, iTunes cards, or some other form of payment card and then read the numbers on the card to the caller.
- This is the only way you can assure that your loved one will be represented and released from law enforcement.
- This is **always** a scam – law enforcement and courts do not demand or accept payment via Green Dot, iTunes, or other prepaid cards.
- **Hang up!**

IRS SCAM

Herald Tribune

- **IRS Scam:** You receive a phone call from someone pretending to be from the IRS telling you that you owe back taxes and if you don’t immediately go purchase Green Dot cards or iTunes cards someone will come to arrest you. The IRS will never phone you and demand immediate payment over the phone nor do they accept payment via Green Dot, iTunes, MoneyGram cards.

IRS SCAM

- **Hang up!** If they contact you by email, never click on a link in the email. That link could install malicious software on your computer that will allow the perpetrator of the scam to gain access to everything on your computer.
  - If you do owe Federal taxes, call the IRS at 1-800-829-1040 and they will help you with a payment plan. If you do not owe taxes, go to the Treasury Inspector General for Tax Administration website and fill out the "IRS Impersonation Scam" form OR call TIGTA at 1-800-366-4484. You may also file a complaint with the Federal Trade Commission. Add "*IRS Telephone Scam*" to the comments in your complaint.

Herald Tribune

MEDICARE SCAM

Medicare Scam:

- You receiver a call allegedly from Medicare telling you that they need your number to issue you a new card or some other reason.

Herald Tribune

MEDICARE SCAM

- Once they have your Medicare number they can begin filing fraudulent medical charges against your number defrauding the Medicare system. Never give that number out over the telephone unless you placed the call to a doctor’s office.

- **Hang up!**

SCAMS 2021

- Zoom phishing emails
- COVID-19 vaccination card scams
- Phony online shopping websites
- Celebrity impostor scams
- *Online romance scams
- Medicare card scams
- Peer-to-peer (P2P) payment scams
- Social Security scam calls
- Account takeover scam texts
- Hotel/Motel Scam
- The pest – Robo Calls

SCAMS 2021

1. Zoom phishing emails

- Con artists registered more than 2,449 fake Zoom-related internet domains in the early months of the pandemic, just so they could send out emails that look like they're from the popular videoconferencing website, according to the Better Business Bureau.

SCAMS 2021

1. Zoom phishing emails

- **The scheme**: “You receive an email, text or social media message with the Zoom logo, telling you to click on a link because your account is suspended or you missed a meeting.”
- “Clicking can allow criminals to download malicious software onto your computer, access your personal information to use for identity theft, or search for passwords to hack into your other accounts.”
- **How to avoid**:
    - Never click on links in unsolicited emails, texts or social media messages. If you think there is a problem with your account, visit Zoom's real website at Zoom.us and follow the steps for customer support.

SCAMS 2021

2. COVID-19 vaccination card scams

- Many who got a COVID vaccine posted selfies on social media showing off their vaccination card. Scammers immediately pounced.
- **The scheme:**
  - "With your full name, birth date and information about where you received your shot, scammers have valuable data for identity theft, breaking into your bank accounts, getting credit cards in your name and more.
- **How to avoid**:
  - If you want to inform friends and family that you got your shots, a selfie with a generic vaccine sticker will suffice.

SCAMS 2021

3. Phony online shopping websites

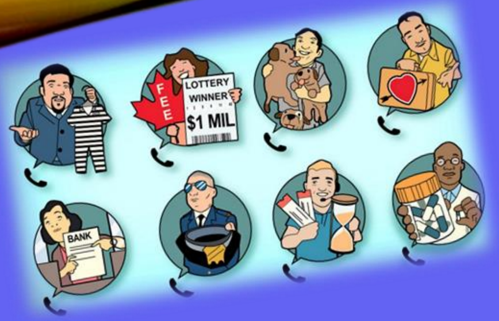
- Phony retail websites aren't new, but they look more real today than ever before.
- "Fake sites are using photos from real online retailers and mimicking their look and feel
- **The scheme:**
    - You click on an ad online or on social media, see stuff you like at a great price, enter your credit card info … and never receive a product.
    - "Or you receive a lower-quality item shipped directly from an overseas seller.

SCAMS 2021

3. Phony online shopping websites

- **How to avoid**: Never click on an ad to go to a retailer's website.
- Instead, bookmark the URLs of trusted shopping websites you visit frequently and use those.
- "Don't bother with trying to figure out whether the web address is real. Attackers adapt and change them frequently."
- If you're considering buying from a new site, first check online reviews as well as the company's track record via the Better Business Bureau's online directory (bbb.org).

SCAMS 2021



4. Celebrity impostor scams

- Real celebs like Kim Kardashian and Justin Bieber grabbed headlines during the pandemic with social media money giveaways.
- Fans posted their cash-transfer app identifier (or $Cashtag, in Cash App) for a chance at free money. Right away, scammers posing as celebrities started offering fake giveaways as a way to get people's private information.

SCAMS 2021

4. Celebrity impostor scams

- **The scheme**: You get a note via social media, email or text message, claiming you won! You just need to verify your account info and send a small deposit up front.

- **How to avoid**:
  - If you really win, you won't be asked to send money first. “The easiest way to defeat this scam is to block incoming requests on your cash-transfer app. Remember: If it sounds too good to be true, it probably is."

SCAMS 2021

Herald Tribune

5. **Online romance scams**

- They're not just lurking on dating sites. “Romance scammers are getting close to unsuspecting women and men in online prayer groups and book groups, through online games like Words With Friends and other groups people are turning to during pandemic isolation.

SCAMS 2021

Herald Tribune

5. **Online romance scams**

- The scheme:
  - Scammers typically lure their romance marks off of sites that may be monitored and onto Google Hangouts, WhatsApp or Facebook Messenger, where no one's watching. Eventually they hit you up for money.

SCAMS 2021

5. **Online romance scams**

- How to avoid:
  - Rule number one: Never send money to someone you've never met in person. And say no to requests for suggestive selfies and videos that a scammer can later use to blackmail you. “It's flattering to be told you are attractive, but it will be used against you.”

SCAMS 2021

6. **Medicare card scams**

- Scammers are emailing, calling and even knocking on doors, claiming to be from Medicare and offering all sorts of pandemic-related services if you “verify” your Medicare ID number.

SCAMS 2021

6. **Medicare card scams**

- The scheme:
  - The offers include new cards they claim contain microchips. Some posers are asking for payment to move beneficiaries up in line for the COVID-19 vaccine.

SCAMS 2021

6. **Medicare card scams**

- How to avoid:
  - Hang up the phone, shut the door, delete the email. According to the Centers for Medicare & Medicaid Services, Medicare will never contact you without permission for your Medicare number or other personal information. And it will never call to sell you anything. Guard your Medicare number and never pay for a COVID vaccine. It's free.

SCAMS 2021

7. **Peer-to-peer (P2P) payment scams**

- The rise of smartphone tools like CashApp, Venmo, Zelle and PayPal, which let you transfer money directly to another person, has led to a range of frauds.

SCAMS 2021

7. **Peer-to-peer (P2P) payment scams**

- The scheme:
  - "One of the more pervasive is the so-called 'accidental transfer of funds' scam,"
    - The Scam is. "A scammer sends hundreds of dollars, then sends a follow-up message requesting the money back, claiming it was 'an accident.' " But the original transfer was made with a stolen debit card; those funds will eventually be removed from your account. And you're out the money.

SCAMS 2021

7. Peer-to-peer (P2P) payment scams

- How to avoid: Scrutinize money requests before hitting “accept.” To be extra diligent, “disable [or block] incoming requests altogether on your app and only use it for sending money.” Enable it when someone you trust is about to send you cash. And ignore a notice to return an accidental deposit. Report the incident to the app's support team to resolve the dispute.

SCAMS 2021

8. **Social Security scam calls**

- Scammers are using “spoofed” phone numbers that look like they're coming from Washington, D.C., to appear credible.

SCAMS 2021

8. Social Security scam calls

- The scheme:
  - You get a scary phone call saying your Social Security number was used in a crime — and you'll be arrested soon if you don't send money to fix it.
  - “They may say your number was used to rent a car where drugs were found and that the Drug Enforcement Agency is on their way to your house,
  - “The caller may refer you to a local law-enforcement website where you can see the person's picture. You think you've checked it out, call them back and send money.”

SCAMS 2021

8. **Social Security scam calls**

- How to avoid: “Don't pick up the phone unless you absolutely know who's calling’
- “If it's important, they'll leave a voicemail.”

SCAMS 2021

9. Account takeover scam texts

- Scammers are sending fake text messages alleging there's big trouble with your internet account, a credit card, bank account or shopping order on Amazon. They want you to click on links and provide personal info.
- The scheme The urgent-sounding text message may have a real-looking logo. “People don't expect scammers to use text messages, so they're more likely to click”.
- How to avoid: Remember, don't click on links in emails and texts that you haven't asked for. Call your bank or credit card company to check for a problem. Installing security software on your computer and keeping it updated is also crucial.

SCAMS 2021

Hotel/Motel Scam

- If you travel and stay at hotels/motels you MUST read this one *Hotel Scam.*
- *Typically when checking in, you give the front desk your credit card (for any charges to your room) and they don't retain the card. You go to your room and settle in.*
- *The hotel receives a call and the caller asks for (as an example) room 620 - which happens to be your room.*
- *The phone rings in your room.*
  - *You answer and the person on the other end says the following: 'This is the front desk. When checking in, we came across a problem with your charge card information. Please re-read me your credit card numbers and verify the last 3 digits numbers at the reverse side of your charge card. '!*

SCAMS 2021

Hotel/Motel Scam

- *' Not thinking anything wrong, since the call seems to come from the front desk you oblige. But actually, it is a scam by someone calling from outside the hotel.*
- *They have asked for a random room number, then ask you for your credit card and address information. They sound so professional, that you think you are talking to the front desk.*
- *If you ever encounter this scenario on your travels, tell the caller that you will be down to the front desk to clear up any problems.*
- *Then, go to the front desk or call directly and ask if there was a problem. If there was none, inform the manager of the hotel that someone tried to scam you of your credit card information, acting like a front desk employee. This was sent by someone who has been duped........and is still cleaning up the mess.*

FCC

ROBO CALLS

- **How to stop:**
  - **Register on the Do Not Call list.**
    - It's free to register at donotcall.gov.
  - **Activate your service provider's free protection.**
    - AT&T, T-Mobile and Verizon offer free services that monitor network activity and crowdsourced reports to block suspected fraudulent calls.
  - **Get a robocall-blocking app**
    - Nomorobo, RoboKiller, Truecaller and YouMail.
  - **Get revenge.**
    - The $4 per month RoboKiller, takes over and fingerprints your voice mails but adds a clever twist — "answer bots."
    - Jolly Roger, doesn't sell itself as a robocall blocker but takes this auto-generated-annoyance idea a step further by actively trying to game the spammers' systems, such as when to press 1 to speak to a human.

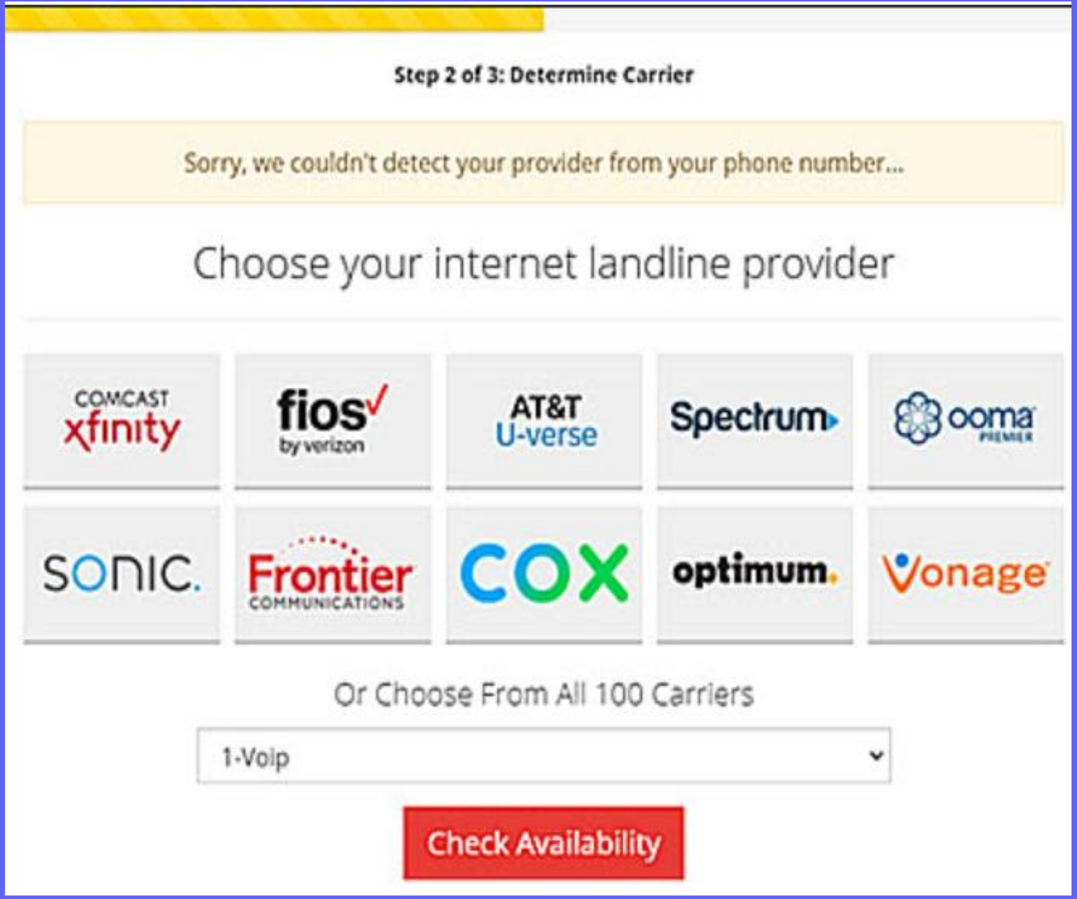
ROBO CALLS

- **Wireless/Mobile**
- AT&T: Mobile security and call protection services.
- Google Project Fi: Call blocking options for Project Fi wireless service.
- Sprint: Call blocking options using My Sprint.
- T-Mobile: Call-protection options to identify or block potential scammers.
- U.S. Cellular: Automatic network call identification, labeling, and blocking app options.
- Verizon: Call Filter FAQS for screening and blocking unwanted calls.

- **Landline/Wireline/VoIP**
- AT&T: Information on Digital Phone Call Protect service, call blocking, and other features.
- CenturyLink: Customer tips and tools to block unwanted calls.
- Comcast: Call blocking options for XFINITY Voice subscribers.
- Frontier Communications: Consumer options for call blocking tools and services.
- Spectrum: Guide for using Nomorobo service to block robocallers.
- Verizon: Customer options for stopping unwanted calls to residential lines.

HOW TO STOP UNSOLICITED ROBOCALLS TO YOUR HOME

- **Set Up Nomorobo**
- Go to https://www.nomorobo.com/signup and follow the instructions for signing up.
    - Choose **Comcast XFINITY** as your landline carrier
    - Step 2. Enter your email address
    - Step 3 and click "**Start Blocking Robocalls Now!**". You'll get an email with a link to activate the Nomorobo service.
    - Step 4 Click on the link and continue as directed.



Step 2 of 3: Determine Carrier

Sorry, we couldn't detect your provider from your phone number...

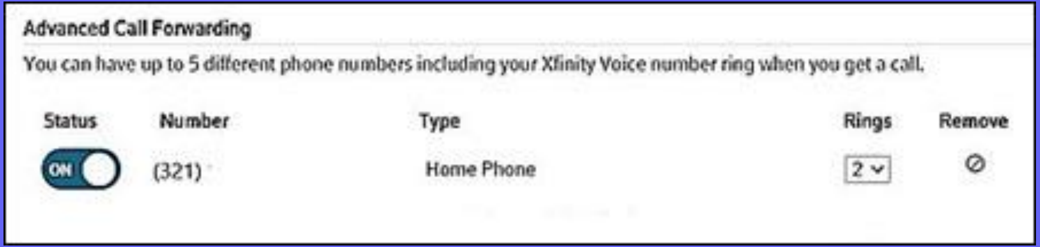
Choose your internet landline provider

Or Choose From All 100 Carriers

HOW TO STOP UNSOLICITED ROBOCALLS TO YOUR HOME

2. When you reach the Setup Your Carrier step on Nomorobo's website.
3. Sign in using your primary Xfinity ID and password, and then select the Voice tab.
4. Click the settings wheel at top right and select Settings.
5. Select Call Forwarding from the menu on the left.
6. Enter the Nomorobo phone number (provided by Nomorobo during setup) into the Advanced Call Forwarding field and select Add.

- Make sure that the Nomorobo phone number is not the only number listed in this section.
- Your number should also be listed as a default. Otherwise, callers may get a busy signal when calling your home phone.
- The number of rings before voicemail should match the rings for your home number. The service automatically terminates calls after one ring.



Advanced Call Forwarding

You can have up to 5 different phone numbers including your Xfinity Voice number ring when you get a call.

Status	Number	Type	Rings	Remove
ON	(321)	Home Phone	2	⊘

HOW TO STOP UNSOLICITED ROBOCALLS TO YOUR HOME

7. After you have completed those steps, go back to the Nomorobo website. Go to **Your Phones** and click the **Test** button next to your number. Then select **I'm ready. Call me now** to perform a test call.
    - You'll get a call to verify that the service is set up correctly. Wait until the **third** ring to pick up the phone.

- Nomorobo will now screen incoming phone calls to your Xfinity Voice telephone number and automatically hang up if a call is determined to be from an illegal robocaller or telemarketer. Your phone will ring once, letting you know that the robocall has been stopped.

- **Disable Nomorobo**
    - To disable Nomorobo, simply return to the **Advanced Call Forwarding** menu (see Step 4 above) and click the **trash icon** next to the Nomorobo phone number.
- **FAQs - *I've enabled and verified Nomorobo on my phone. What do I do now?***
- Continue to use your phone like normal. All you'll need to do is to wait for the second ring to answer the phone for incoming calls, as Nomorobo needs the first ring to detect robocallers. If you only hear one ring and then it stops, you know a robocaller was just blocked. If the phone continues ringing, you can answer it.

ROBO CALLS

- **Third-Party Analytics Resources**
- First Orion: Tools and services for mobile customers and businesses.
- Hiya: Tools and services for mobile phones; Hiya Connect for businesses.
- Nomorobo: Tools and services for VoIP landlines and mobile phones.
- TNS Call Guardian: Call analytics solutions for businesses.
- YouMail: Tools and services for individuals and businesses.

- **Wireless Device Solutions**
- Apple iPhones have an opt-in "Silence Unknown Callers" call-screening and blocking feature.
- Google Pixel phones have a "Call Screen" call-screening and blocking feature; Google offers several free, opt-in, call-blocking tool apps for Android phones; and Google Voice users can use a call management tool to block unwanted calls.
- Samsung partners with Hiya to offer a call-blocking solution called Smart Call to label potentially unwanted calls.

STOP IDENTITY THEFT

PREVENT IDENTITY THEFT

- Check your credit report regularly.
- Shred unsolicited credit card applications.
- Monitor your account statements for unauthorized transactions.
- Follow up with creditors if you bill s are missing.
- Keep your Social Security card and number in a safe location.
- Do not respond to spam email

WHAT CAN YOU DO IF YOU'VE BECOME A VICTIM OF IDENTITY THEFT?

- Call the companies where you know the fraud occurred.
  - Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
  - Change logins, passwords, and PINs for your accounts.

WHAT CAN YOU DO IF YOU'VE BECOME A VICTIM OF IDENTITY THEFT?

- To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
    - Experian.com/fraudalert 1-888-397-3742
    - TransUnion.com/fraud 1-800-680-7289
    - Equifax.com/CreditReportAssistance 1-888-766-0008
- A fraud alert is free. It will make it harder for someone to open new accounts in your name.
- Get your free credit reports from Equifax, Experian, and TransUnion. Go to annualcreditreport.com or call 1-877-322-8228.
- Review your reports. Make note of any account or transaction you don’t recognize. This will help you report the theft to the FTC and the police.

WHAT CAN YOU DO IF YOU'VE BECOME A VICTIM OF IDENTITY THEFT?

Report identity theft to the FTC.

- Go to IdentityTheft.gov or call 1-877-438-4338. Include as many details as possible.
- Based on the information you enter, IdentityTheft.gov will create your Identity Theft Report and personal recovery plan.

WHAT CAN YOU DO IF YOU'VE BECOME A VICTIM OF IDENTITY THEFT?

You may choose to file a report with your local police department.

- Go to your local police office with:
  - A copy of your FTC Identity Theft Report
  - A government-issued ID with a photo
  - Proof of your address (mortgage statement, rental agreement, or utilities bill)
  - Any other proof you have of the theft—bills, Internal Revenue Service (IRS) notices, etc.
- Tell the police someone stole your identity and you need to file a report.
- Ask for a copy of the police report. You may need this to complete other steps.

SUMMARY OF PART ONE

Some of the common identify frauds are:

- Criminals see or hear you personal information.
- Criminals find your info in the trash.
- Most of the time the fraud is committed by phone, email, or internet.
- Criminals want your drivers license, social security number, Medicare number, your name, your banking credit card numbers and other financial account information.

SUMMARY OF PART ONE

They use this info to perpetrate:

- Mortgage Fraud
- Credit and Debit Card Fraud
- Prize and Lottery Fraud
- Debt Collection Fraud
- Covid 19 Scam
- Grand Child Scam
- IRS Scam
- Jury Duty Scam
- Fake Check Scam
- Computer Repair Scam
- Medicae Scam
- Fake Charity Scam

SUMMARY OF PART ONE

- **You Should: “The big 5”**
  1. Check your credit card statements frequently.
  2. Check the three credit bureaus frequesntly.
  3. Never give info over the phone if you did not make the call.
  4. Hang up on anyone who says you are getting money or owe money, then call the police!!! (we are to gullible)
  5. Do not click on attachments, and keep an eye on what websites you are really on.
- If you see a problem:
  - Contact banks and cannel cards/lock accounts.
  - File report with FTC.
  - File report with Police.

HOW DO I PROTECT MY COMPUTER AND MY DATA

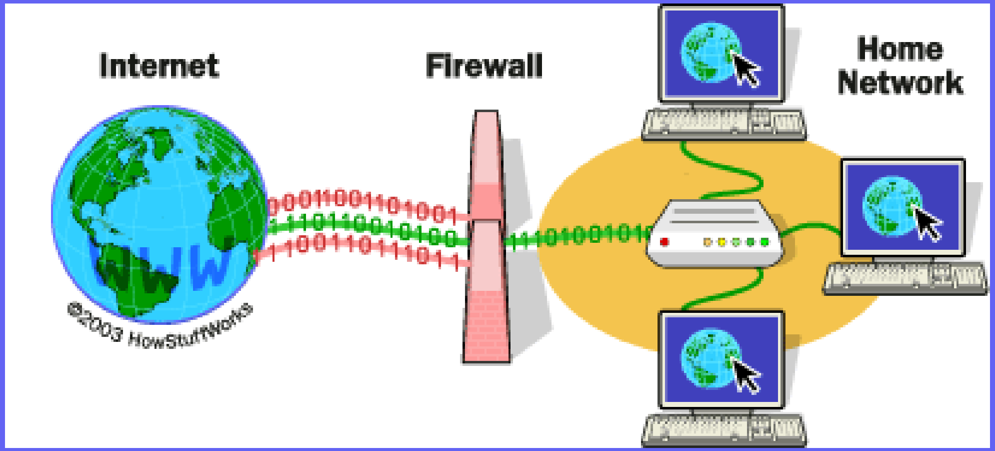
PROTECT MY COMPUTER AND MY DATA

- Firewall.
- Virus protection.
- Update your applications and Operating system.
- Have “STRONG” passwords.
- Watch what you click on.
- Attachments are not your friends.
- Beware of computer scams.
- What info are you putting out there?
- Backup your information.

PROTECT YOUR COMPUTER AND YOUR DATA

FIREWALL

- What is a Firewall
  - A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.



FIREWALL

- Hardware
  - Modem with Passcode
    - Incoming check
- Software
  - Windows Firewall – Windows Defender for w10 –
    - Two-way network traffic filtering

MALWARE

- What is Malware?
  - The term *malware* is a contraction of malicious software. Put simply, *malware* is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, Trojans, spyware, and ransomware are among the different kinds of *malware*.

TYPES OF MALWARE

- Adware --- (short for advertising-supported software) is a type of malware that automatically delivers advertisements.
  - Common examples of adware include pop-up ads on websites and advertisements that are displayed by software.
- Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom.
- A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs.
- A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware.

TYPES OF MALWARE

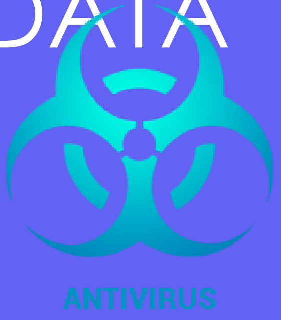
- A virus is a form of malware that is capable of copying itself and spreading to other computers.
- Computer worms are among the most common types of malware.
  - They spread over computer networks by exploiting operating system vulnerabilities.
  - Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers.
- **Spyware is a type of malware that functions by spying on user activity without their knowledge.**
  - **It transfers what it finds on your computer back to the originator.**
- Spam is the electronic sending of mass unsolicited messages.

MALWARE SYMPTOMS

- Increased CPU usage.
- Slow computer or web browser speeds.
- Problems connecting to networks
- Freezing or crashing.
- Modified or deleted files.
- Appearance of strange files, programs, or desktop icons.
- Programs running, turning off, or reconfiguring themselves (malware will often reconfigure or turn off antivirus and firewall programs).
- Strange computer behavior.
- Emails/messages being sent automatically and without user's knowledge (a friend receives a strange email from you that you did not send).

PROTECT YOUR COMPUTER AND YOUR DATA

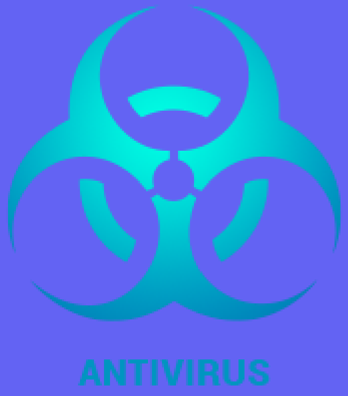
- Antivirus
  - Can prevent known viruses from getting on your computer.
  - It can not prevent all viruses. You can get one by clicking the wrong place while on the internet.
  - The antivirus program needs to be running all the time and updated constantly.
  - You also need to scan your system with the antivirus program in case a virus got through.



PROTECT YOUR COMPUTER AND YOUR DATA

- Some good Antivirus programs for PC's are:
  - TOTAL AV (free)
  - Scan Guard
  - Pcprotect
  - Bitfinder (free)
  - Norton
  - Malwarebytes* (free)
  - AVG (free)
  - Avast* (free)
  - McAfee
  - MSE - Microsoft Security Essentials *
  - Windows Defender

- Some good Antivirus programs for MAC's are:
- Norton
- McAfee
- Kaspersky
- Panda
- Bull Guard
- ESET
- Avira
- Avast
- AVG



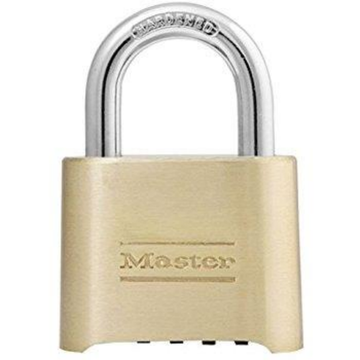
KEEP IT UP TO DATE

- Keep the major features of your device up to date.
  - The Operating System.
  - The Antivirus and Spyware Software.

PROTECT YOUR COMPUTER AND YOUR DATA

- Scams
  - Internet scams –
    - If it is to good to be true. IT IS!!
    - If you get strange messages or videos and voices that will not stop. (**call this number at once or go to this web site**)
      - Turn off your browser.
      - Or shut down your computer.
      - Or push and hold the power button to do an emergency power down.

PASSWORDS ARE THE KEYS AND COMBINATION TO THE COMPUTER WORLD



PASSWORDS:
THE THING WE HATE THE MOST AND NEED TO LEARN TO LOVE.

We use passwords for a lot of things.

- To access our devices.
  - Computer
  - Phone
- To access internet sites.
  - Banks
  - Email
  - Shopping

What is Two Factor Authentication?

- Requiring something in addition to a password to get to what you want to do.

PASSWORDS:
THE THING WE HATE THE MOST AND NEED TO LEARN TO LOVE.

Creating passwords.

- Keep Passwords Strong.
  - At Least Eight Characters.
  - At least one Capital letter.
  - At least 1 number.
  - At least on special character like ! , ~, $, #, @, %
- **Write Them Down!!!!!!!!!**

PASSWORDS

- You only need THREE CORE passwords.
    - Examples are - gr8HØusE@ or 4g3tMe!$ or sKØØlskoob~
- Have a truly unique password for your banking.
- Have another unique password for all your email addresses.
    - If one gets compromised, change the password for all your email addresses.
- Have another that can be adapted for all other websites.
    - Example - if your master password is gr8#SocKs, then the password for Facebook would be Fgr8#SocKs, or fbgr8#SocKs
- Make these changes over time. Not all at once. Set a target of a week or two. Or the next time you log into that site.
- **Write Them Down.**

INTERNET BROWSING IS A MAJOR WAY TO GET VIRUSES

- Use one of the major internet browsers.
  - Edge, Internet Explorer, **Firefox**, Chrome, Safari, **Vivaldi**.
- Use one of the major search engines.
  - Google, Bing, Yahoo, **Duck Duck Go, Startpage**.
- Don’t allow website to save cookies.
  - This can be set in options or setting in the browser you are using.
  - An exception would be your financial institution.

INTERNET BROWSING IS A MAJOR WAY TO GET VIRUSES

- Surfing
  - Do not go to websites you do not recognize. (know where you are)
    - **Check the address bar** to see if you are on the website you want to be on and if it is secure.
  - Example: www.google.com
  - When using a search engine, the first page of the web sites , resulting from a search, are usually ok. More then that could be suspect.
  - Some browsers, search engines, and email programs will warn you about potential fraudulent or problem

INTERNET BROWSING

- Unlink accounts:
  - You may be asked if you will allow a web account to link to another account you already have. While this is convenient, do not do it.
- Don’t believe sweepstakes in browser or email.
  - If it is too good to be true it is fake.

INTERNET BROWSING

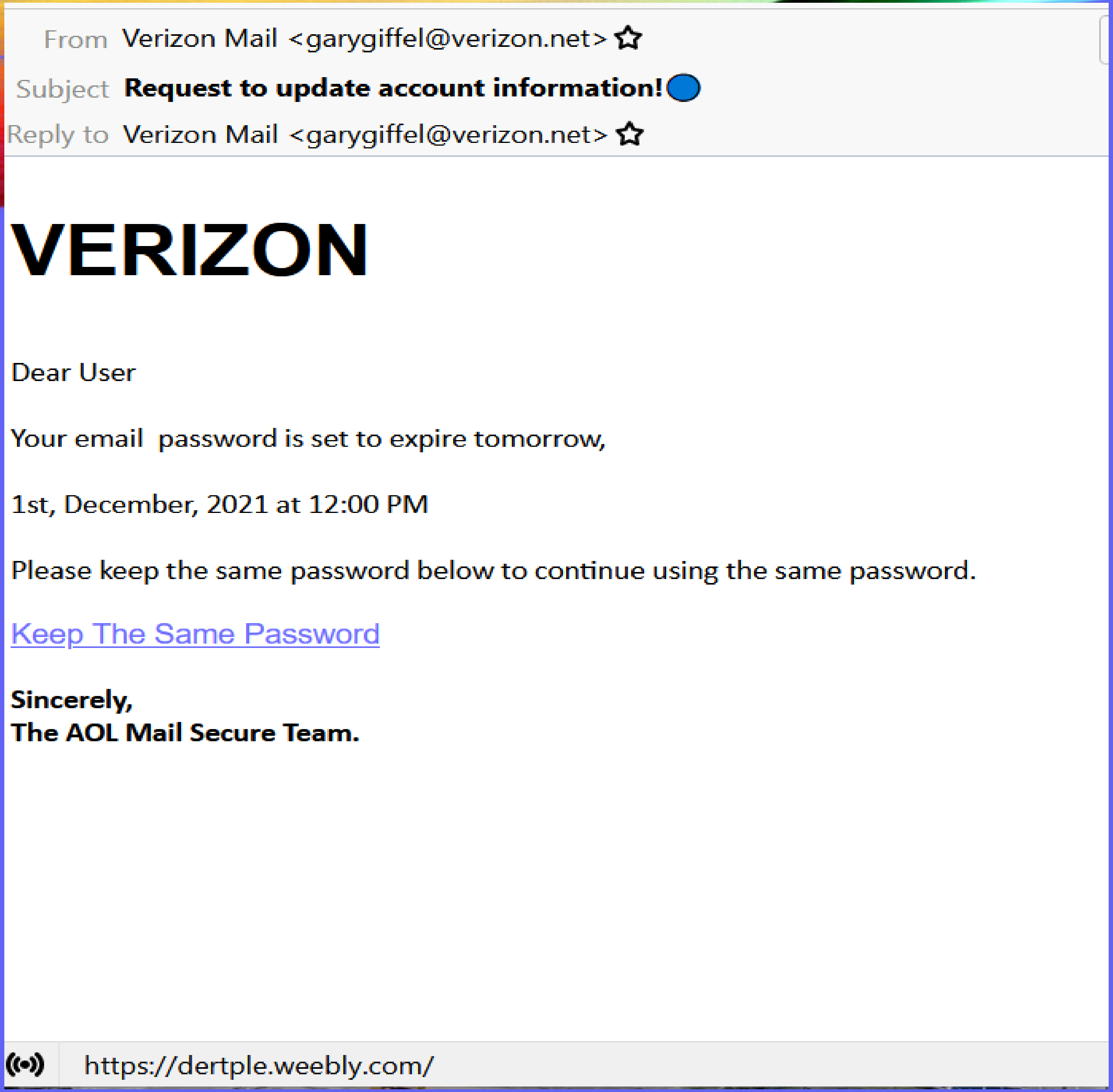
- When to click:
  - As you are looking over a web site you may click on something and suddenly something happens.
  - When this happens close your browser and start over.
- Watch your finances.
  - Check your banking account frequently to insure there is no unauthorized activity.

EMAIL IS ANOTHER PLACE TO GET VIRUSES AND MORE

- Phishing -
  - No legitimate business will ask you to go to their web site to update or check your account.
  - Go to the account directly, do not use the link, to see if there is something to do.
  - Links take you places you do not expect.

Email – Attachments and Links

- Attachments open something on your computer
    - They are a major source of viruses and spyware.
    - Unless you are very sure of a attachment, do not click on it.
- Links take you to a web sight.
    - They may not be taking you to where they say.
    - Where does this link take you? bing.com



From Verizon Mail <garygiffel@verizon.net> ☆

Subject **Request to update account information!🔵**

Reply to Verizon Mail <garygiffel@verizon.net> ☆

VERIZON

Dear User

Your email password is set to expire tomorrow,

1st, December, 2021 at 12:00 PM

Please keep the same password below to continue using the same password.

Keep The Same Password

Sincerely,
The AOL Mail Secure Team.

https://dertple.weebly.com/

EMAIL SCAM

EMAIL

- Scams -
  - If it is too good to be true it is fake.
- Avoid unknown emails.
  - Delete an email if you do not know the source.
- Junk Mail –
  - If you try to unsubscribe you may be setting yourself up for more junk mail.
- Get two email addresses:
  - One for family and friends.
  - One for everywhere else you are asked for you email address.
    - Most of those just want to send you junk or sell your address to others that will send you junk.

GIVING AWAY YOUR IDENTITY

- You are giving away your identity every time you register for using a program
  - Face book
  - Instagram
  - Google
  - Twitter
- You are giving away more of your identity every time you use one of these programs
  - Google - maps,search,photos
  - Amazon - music, purchases
  - Facebook - friends, likes, and much more

APPLICATIONS SHARE YOUR DATA

- If an application shares your data. It can share
  - Contacts
  - Location
  - Applications you use
  - Your music
  - Your demographics
  - Your search history
  - What products you buy

PRIVACY INFORMATION AND SETTINGS

- FACEBOOK, GOOGLE, TWITTER, INSTAGAM are all social media sites that want as much personal data as they can get and want to share it with as many folks as they can.
  - Give then as little info as you can.
  - Use all the settings they give you - request them to share as little of your information as you can.

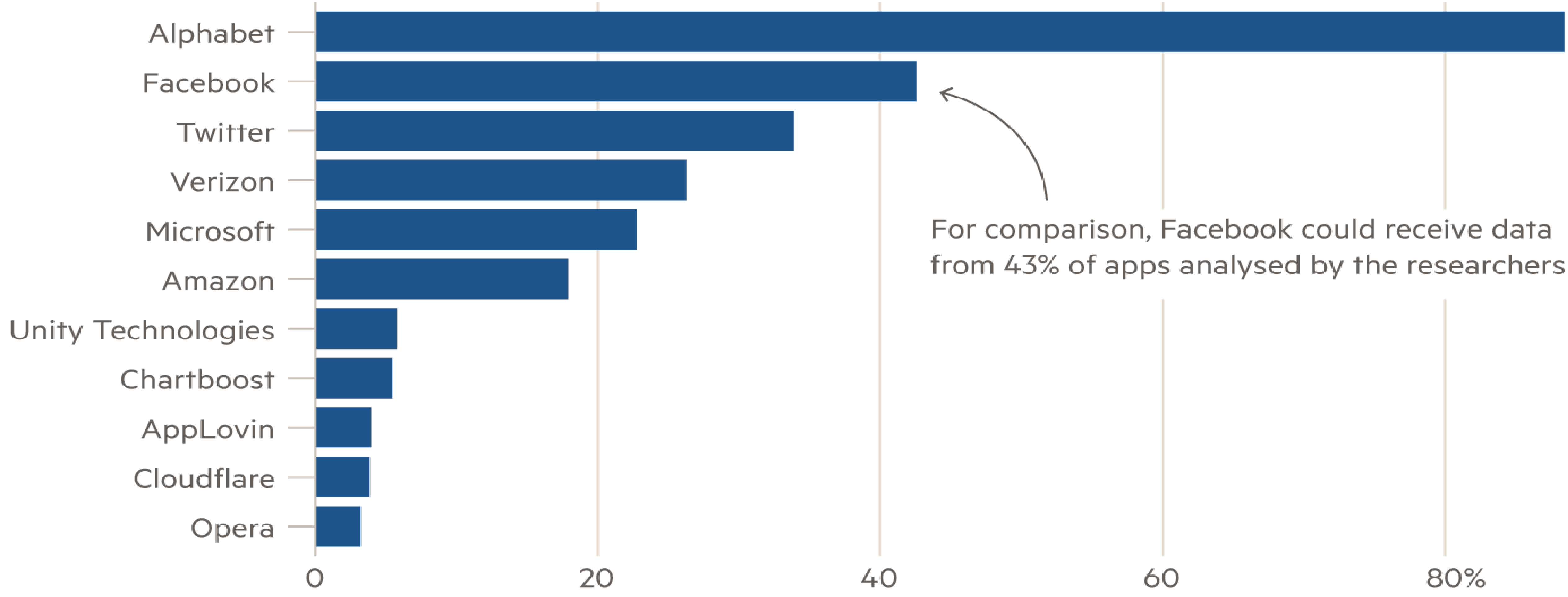
FACEBOOK

- What is the minimum information needed to great a Facebook account.
    - Your age. (must be at least 13)
    - Your real name
    - Sex
    - Email address
    - Mobile phone number if account is created on a mobile phone.
    - Password

- Not needed are but requested:
    - Photo
    - Profession
    - Favorite films
    - Pets names
    - Town where you went to high school
    - University or College
    - Business name
    - Places you have lived
    - Websites
    - Other Email addresses
    - Family relationships
    - Nicknames
    - Life events
    - Friends

Smartphone data flows to the world's biggest tech companies

Data from more than 88 per cent of apps in the study could end up with Alphabet



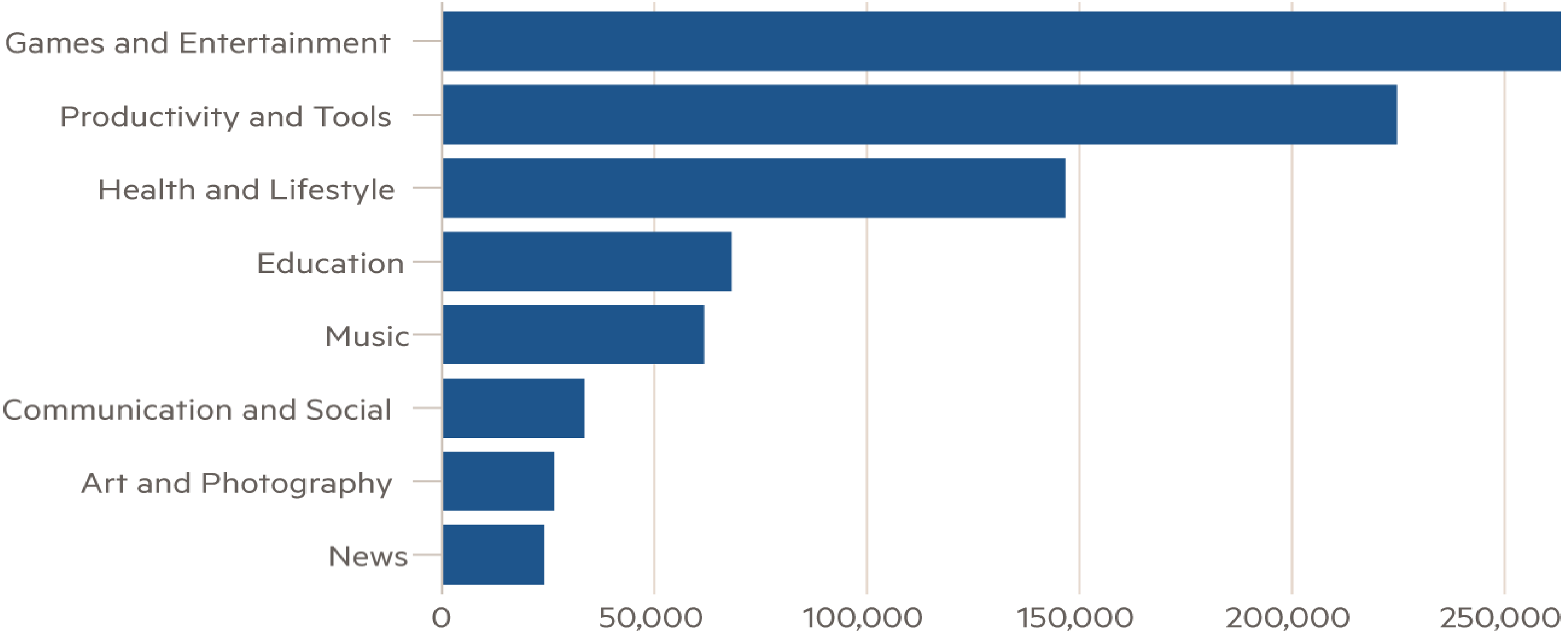
For comparison, Facebook could receive data from 43% of apps analysed by the researchers

Source: Third Party Tracking in the Mobile Ecosystem, October 2018

© *FT*

Alphabet dissected

Apps set up to send data back to Google and other Alphabet subsidiaries



Source: Third Party Tracking in the Mobile Ecosystem, October 2018

© FT

GOOGLE

- Search
- Mail
- Contacts
- Maps
- YouTube
- Play -Games
- Drive - Storage
- Calendar
- Shopping –like Amazon
- Translate
- Photos
- Chrome - Browser
- Duo – video chat

- Finance – Banking and investments
- Docs - like Word
- Books
- Blogger - create a Blog
- Hangouts - video, text,voice chats
- Slides – like Powerpoint
- Sheets – like Excel
- Keep – note taking
- Chat- messaging
- Meet – video meeting
- Jamboard – Shared whiteboard
- Collections - like pinterest

- Earth
- Google ads
- Podcasts
- Stadia – game playing center
- Google one – Cloud storage
- Travel travel plans and bookings
- Forms
- Classroom – stream line the sharing of files between teacher and student.

clario.

The companies that know most about you

#	Company	% of personal data collected	Email	Name	Age	Gender/Sex	Sexual Orientation	Marital Status	Race	Religious Belief	Live Location	Home Address	Employment Status	Job Title	Pet/Animal Ownership	Mobile Number	Landline Number	Type of Phone/Device	Hobbies	Interests	Height	Weight	Next of Kin	Mother's Maiden Name	Current Employers	Past Employers	Bank Account Details	Salary	Social Profile (Friends)	Social Profile (Hobies)	Social Profile (Interests)	Country of Birth	Allergies/Intolerances	Health & Lifestyle Info
1	Facebook	70.59%	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●		●	●			●	●	●			
2	Instagram	58.82%	●	●	●	●					●	●	●	●	●	●		●	●	●	●	●			●	●			●	●	●			
3	Tinder	55.88%	●	●	●	●	●	●			●		●	●	●	●		●	●	●	●						●		●	●	●			
4	Grindr	52.94%	●	●	●	●	●	●			●		●	●	●	●		●	●	●	●								●	●	●			
5	Uber	52.94%	●	●	●	●					●	●	●	●		●	●	●	●	●						●	●		●	●	●			
6	Strava	41.18%	●	●	●	●					●	●				●		●			●	●					●		●	●	●			
7	Tesco	38.24%	●	●	●	●		●				●				●	●	●									●		●	●	●			
8	Spotify	35.29%	●	●	●							●				●	●	●		●							●		●	●	●			
9	MyFitnessPal	35.29%	●	●	●							●				●	●	●			●	●					●						●	
10	Jet2	35.29%	●	●	●	●		●	●			●				●	●	●									●					●		

HOW DO YOU PROTECT YOUR IDENTITY AND YOU FINANCES WHILE USING TODAY'S TECHNOLOGY?

- What About Non Computer/Phones /Tables?
- Backup

FOLLOW THESE STEPS TO TAKE BACK YOUR PRIVACY

- On **iPhone**:
  - Open the **Settings** app.
  - Scroll down and tap the **Privacy** icon.
  - Select a permission, like **Calendar**, **Location Services**, or **Camera**.
  - Choose which apps should have access to that permission and remove the permissions for the apps you don't want to have access.
- On **Android**:
  - Open the **Settings** app.
  - Tap **Apps & notifications**, followed by **Advanced App permissions**.
  - Select a permission, like **Calendar**, **Location**, or **Phone**.
  - Choose which apps should have access to that permission and remove the permissions for the apps you don't want to have access.

WHAT ABOUT NONE COMPUTER/PHONES /TABLES?

- In addition to Smart Phones and Tablets there are more and more Home devices the are internet enabled.
    - Many of the new things you get for the home are internet enabled.
        - AC/Heat controls, Lights, Video cameras, Door Locks.
        - Echo, Dot (they are listening)
        - CPAP Machines.

BACKUP

- **<u>Your computer system will fail.</u>**
- Everyone should backup the information they do not want to lose and/or you would like to use on your new computer.
  - Pictures
  - Documents
  - Music
- You can not backup programs.
- You can back up the entire system.
  - System image or system back-up
- Email does not need to be backed up and your banking info is with the bank.
    - Exception would be Quicken data.
- The process can be as straight forward as copying your information to a flash drive once a week or once a month.

BACKUP PROGRAMS

- Computer Based – save the info locally.

Acronis True Image 2019	$49.99
Aomei Backupper	$0.00
EaseUS ToDo Backup Home 10.5	$29.99

- Cloud backup

iDrive	$13.99/yr
BackBlaze	$50/yr
Carbonite	$71.99/yr
Acronis	$49.99/yr

FOR PRIVACY:

- Use **ProtonMail** approx. $50/year.
- Use **Parlor** for your tweaking
- Use **BRAVE** for you Browser
- **DUCKDUCKGO** or **Startpage** for your search engine.
- Use **Signal** for messaging.
- Do not link sign-ins for applications
- Use **NordVPM for your** VPN.

PLEASE NOTE

- Although anyone can become a victim, the elderly are especially vulnerable to scams. If you believe that you or your parent have fallen victim to a scam, report it to your local police department.
- Caregivers, those holding powers of attorney, family, and friends can potentially exploit the elderly.
- Keep track of bank statements and financial documents, review them regularly, and report any discrepancies to your bank or credit card company immediately.
- If money has disappeared from your account, file a report with your local police department.

THE BOTTOM LINE

- It’s safe to assume that if anyone is asking for your bank or personal information, you’re being scammed. You should never give out personal information to anyone on the internet who contacts you directly.
  - If you have to make a financial transaction online, make sure you’re doing so on a secure server and through a reputable site.
- If you believe you’ve been scammed, immediately change all of your passwords and delete any malicious software you may have downloaded, and call your credit card company, if necessary.
  - Contact your local law enforcement authorities to report the scam and get help with the next steps.
  - You can also report the scam to the Federal Trade Commission.

THAT'S IT.
TO AVOID IDENTITY AND DATA THIEF:

- Do not fall prey to phone or internet scams that are after your identity.
- Be sure you have a software and hardware firewall.
- Use good antivirus software and keep it updated.
- Have 3 basic passwords that are somewhat complex.
- Be very careful with email.
  - Do not open most attachments.
  - Watch the links that you may click on.
- Be careful, aware, and wary about where you go on the internet.
  - Watch the address bar.
- Back up your data in case of disk failure or Ransomware.

STAY SAFE
MY FRIENDS
memecrunch.com

QUESTIONS?