PROTECTING YOUR COMPUTERS, CELL PHONES, AND YOU FROM MALWARE AND SCAMS

COMPILED BY HOWIE BAUM

INTRODUCTION

The digital world should be a place of convenience and connection, not fear.

We'll explore the basics of digital security, from recognizing tricky scams to keeping your devices clean from malware.

By the end of this session, you'll have the tools and knowledge to protect yourself, your finances, and your peace of mind while using your computer and cell phone.

SECURITY MINDSET

Protecting our lives and our property

- Locking doors
- Checking who is at the door
- Alarm systems
- Washing your hands
- Leaving a light on
- Firesafe for valuables

- Become aware of the threats
- Initiate behaviors to minimize threats
- Take steps to prevent attacks
- Protect your self and others

...I barely use the Internet
...I don't shop/bank online
...I don't have anything to steal
...That's what the IT person is for

CYBERSECURITY – IT AFFECTS EVERYONE

- We are more connected than we realize
- Your information is valuable
- 95% of all Cyber Security Breaches are caused by human mistakes and misunderstanding
- It doesn't just affect you

STATISTICS ABOUT THE FINANCIAL AND ASSET-RELATED LOSSES, FROM COMPUTER USE

🧠 General Cybercrime & Internet Fraud

$16.1 billion in reported losses from internet crime in the U.S. in 2024—a 33% increase from 2023
.
Investment fraud involving cryptocurrency accounted for over **$6.5 billion** in losses in 2024
.
People over age 60 suffered nearly **$5 billion** in losses—more than any other age group .

🛍️ Consumer Fraud & Scams

The FTC reported **$12.5 billion** in consumer fraud losses in 2024—a 25% increase from 2023 .

38% of fraud victims reported losing money in 2024, up from 27% in 2023 .

Investment scams led all categories with **$5.7 billion** in losses, followed by **imposter scams** at **$2.95 billion**
.
Government imposter scams rose by $171 million in one year, totaling **$789 million** in 2024 .

💼 Job & Business Scams

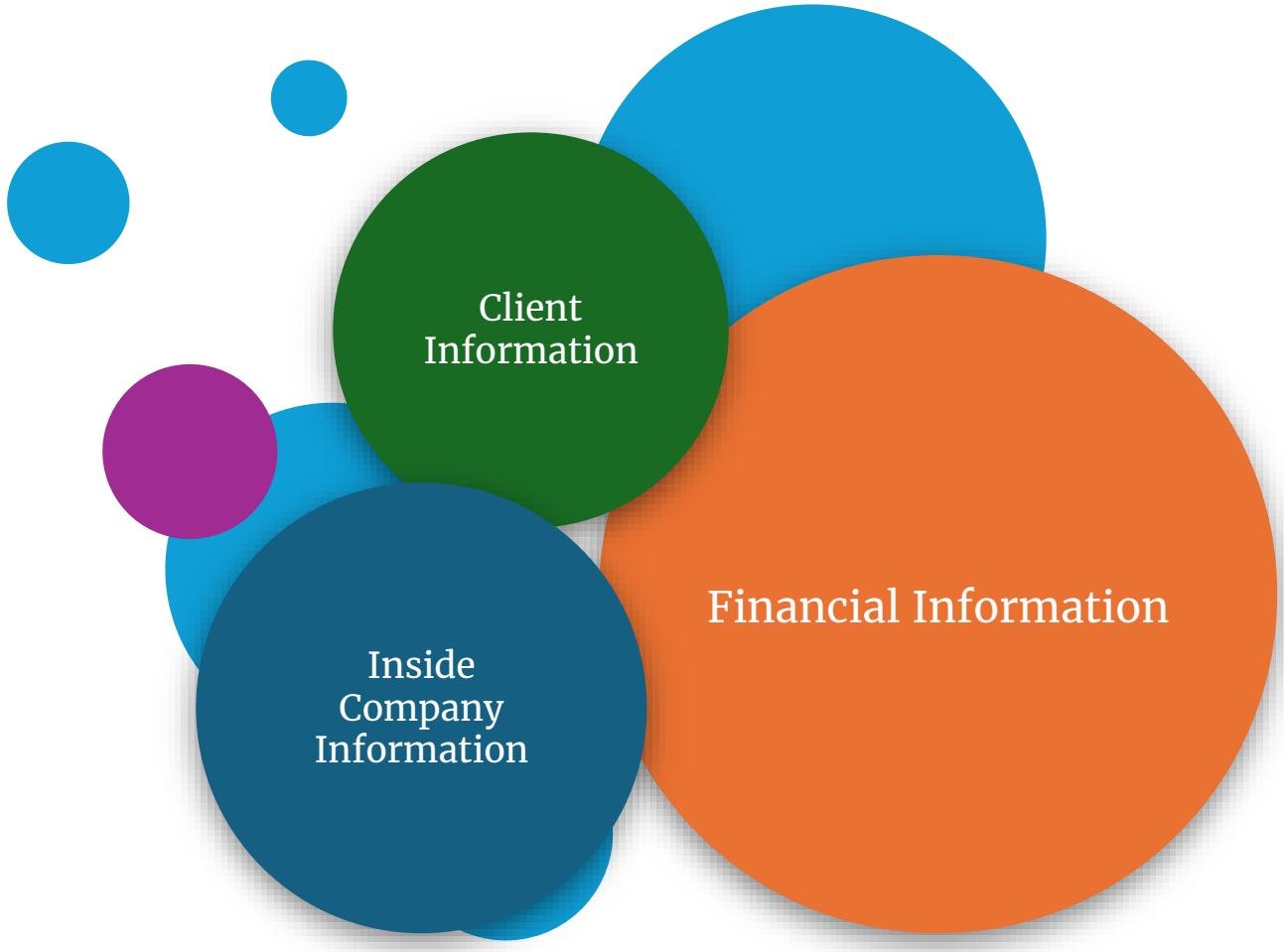
Losses from **job and employment agency scams** jumped from **$90 million in 2020** to **$501 million in 2024** .

Confidential Information

Some information is more sensitive than others.

Confidential Personal Information

Confidential Work Information



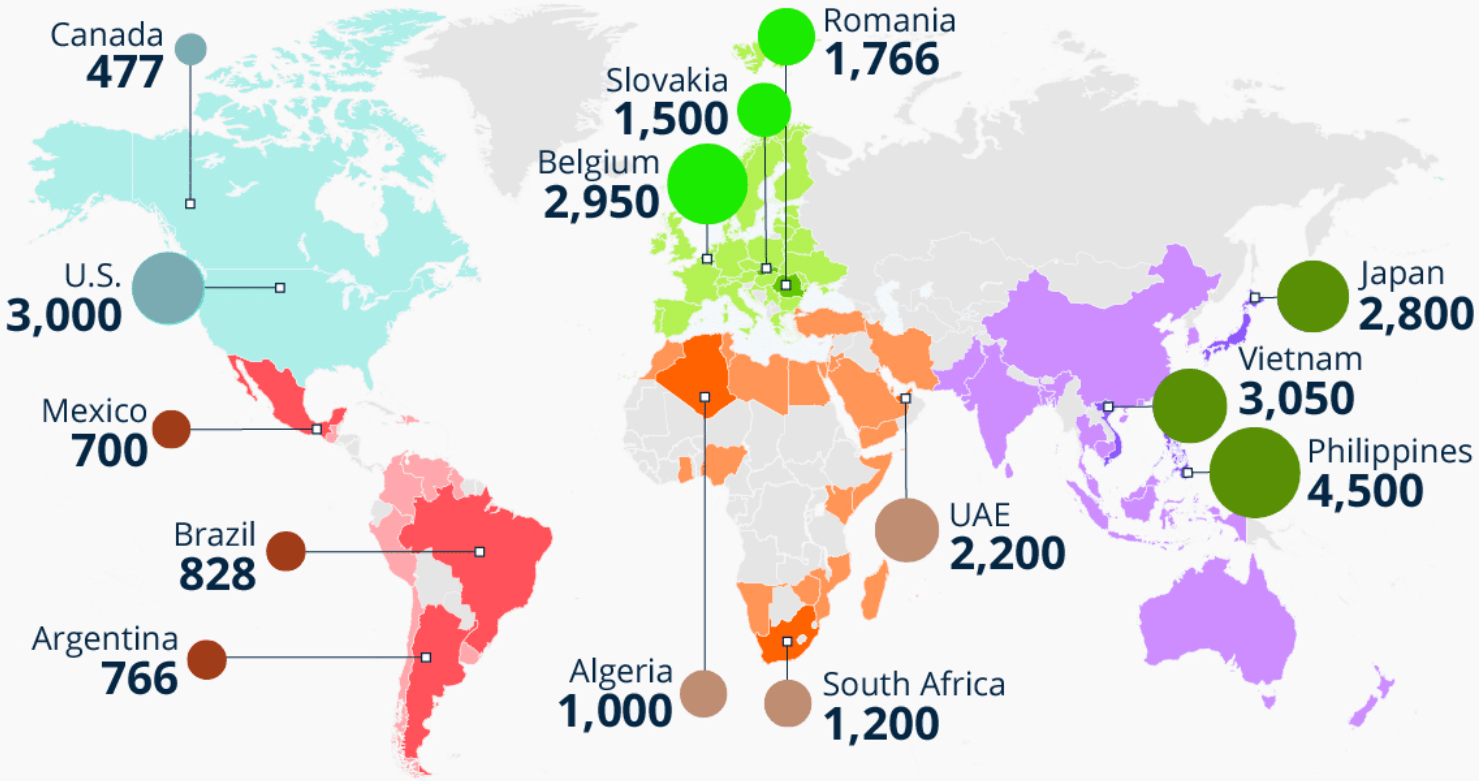
Keep Confidential information Secure

- Never send confidential information through email.
- Use extreme caution when providing confidential information to a website.
- Keep your confidential information in a secure location.

bright defense

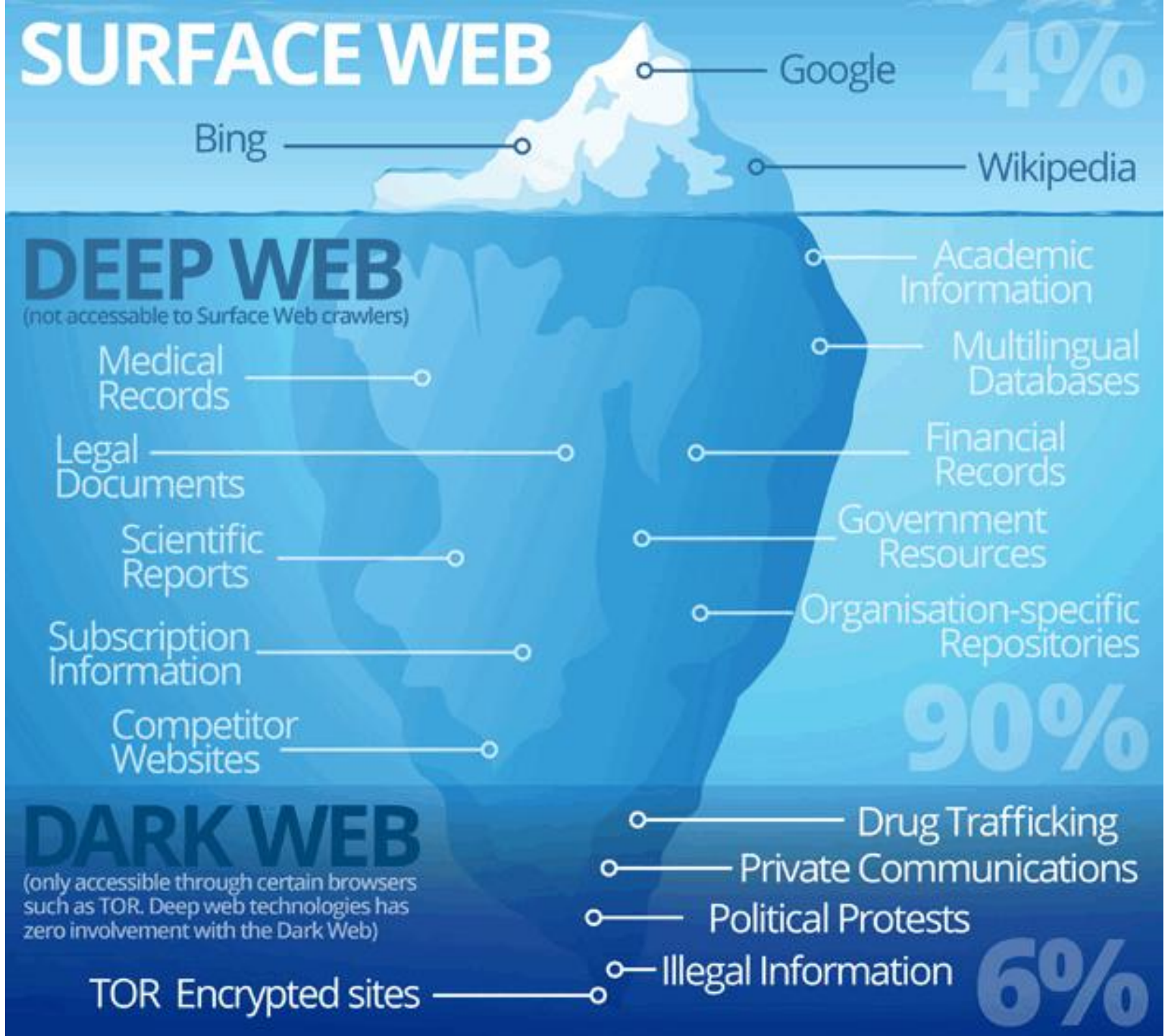
AI-FUELED FRAUD IS SURGING FAST

TOP COUNTRIES BY REGION SHOWING THE SHARPEST RISE IN DEEPFAKE-RELATED FRAUD FROM 2022 TO 2023 (PERCENTAGE GROWTH)*



The report examines over 2 million identity fraud attempts across 224 countries and territories.All data has been aggregated and anonymized. *Regional classification based on the source.
Source: Sumsub Identity Fraud Report 2023

> IF THE CYBERCRIME INDUSTRY WERE A COUNTRY, IT WOULD RANK AS THE THIRD-LARGEST ECONOMY IN THE WORLD, RIGHT BEHIND THE US AND CHINA.

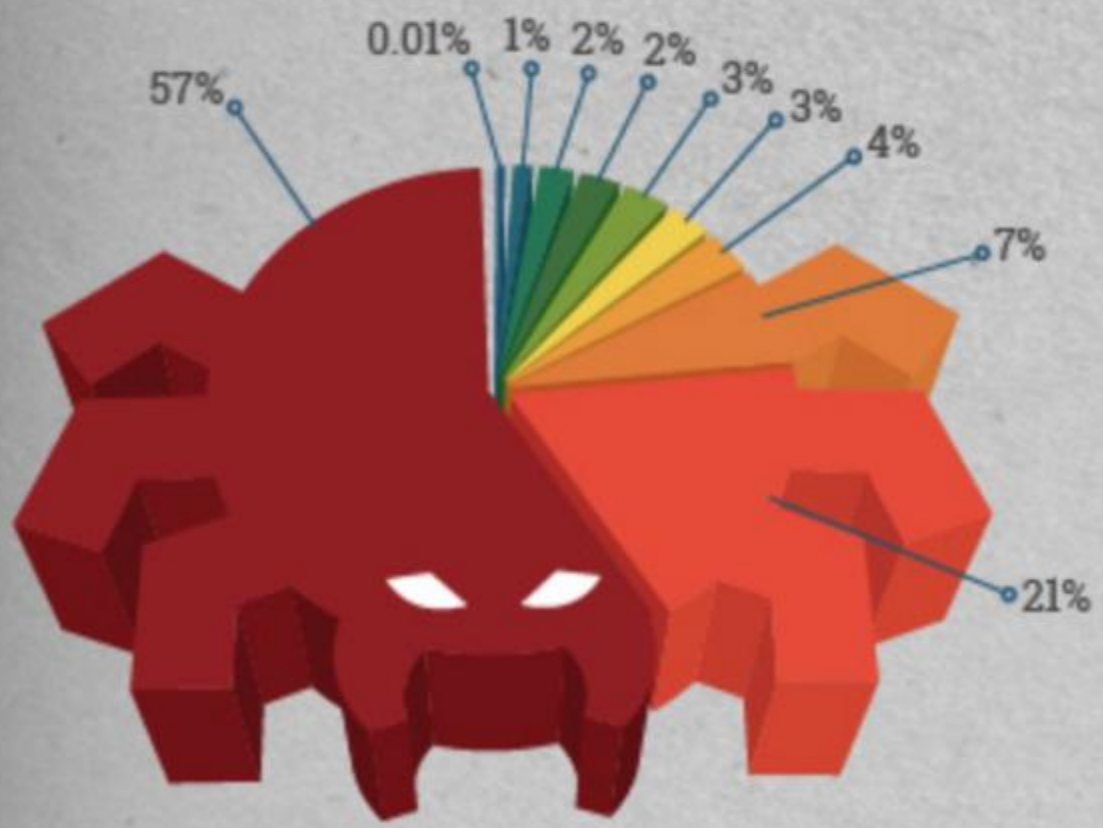

SURFACE WEB
Google
4%
Bing
Wikipedia
DEEP WEB
(not accessable to Surface Web crawlers)
Academic Information
Multilingual Databases
Medical Records
Financial Records
Legal Documents
Government Resources
Scientific Reports
Organisation-specific Repositories
Subscription Information
90%
Competitor Websites
DARK WEB
(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)
Drug Trafficking
Private Communications
Political Protests
Illegal Information
TOR Encrypted sites
6%

Malware, Viruses, Spyware, and Ransomware

Oh My!

12 common types of malware

(Annoying Popups) Adware

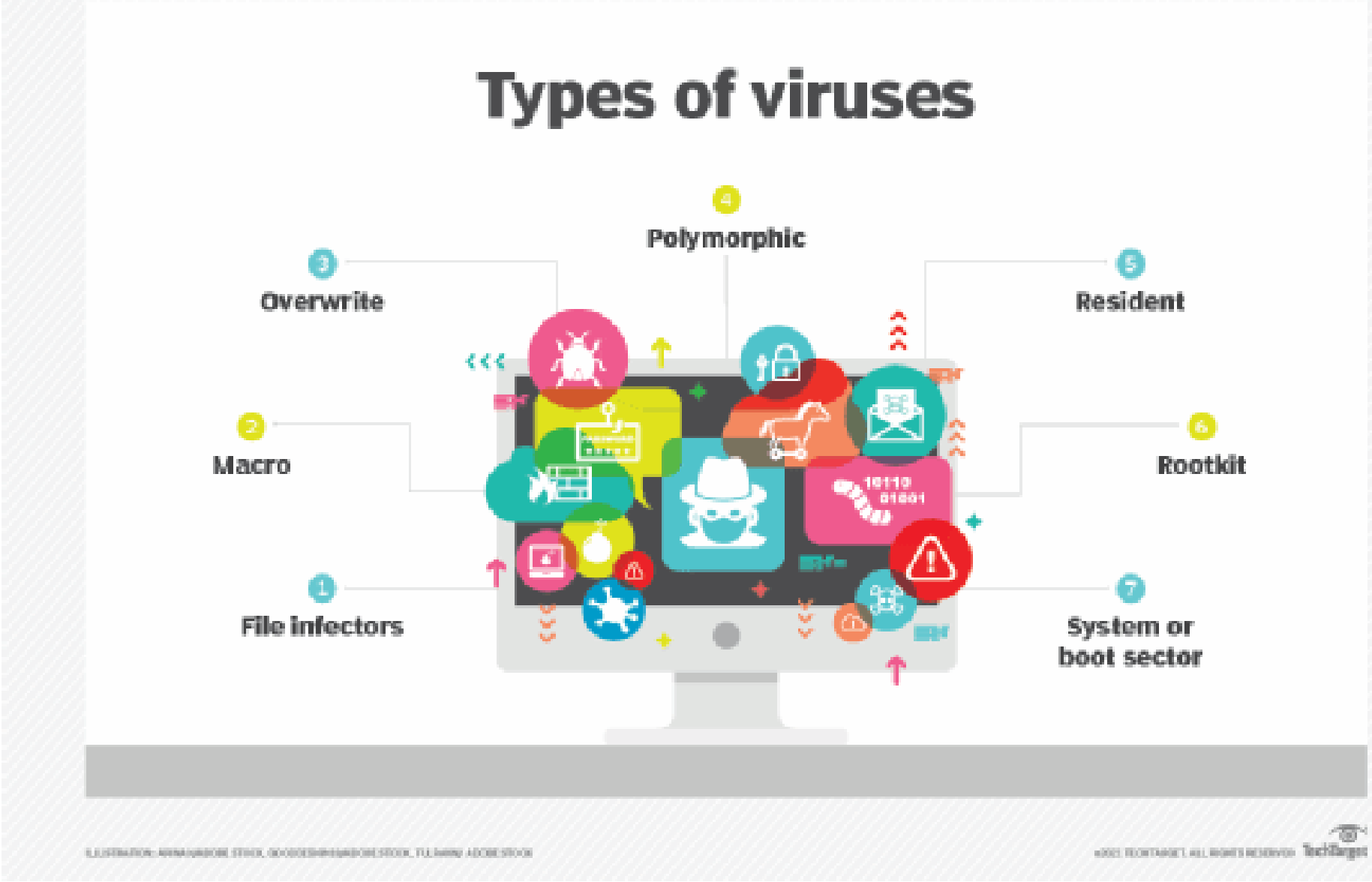


Viruses	57%
Misc. Trojans	21%
Trojan Downloaders	7%
Misc. Unwanted Software	4%
Adware	3%
Exploits	3%
Worms	2%
Monitoring Tools	2%
Back Doors	1%
Spyware	0.01%

57%

vi·rus

A form of malware that is capable of copying itself and spreading to other files via many various user actions.



COMPUTER PROGRAMS THAT REPRODUCE AND INFECT OTHER COMPUTERS

TYPES OF MALWARE

Type	What It Does	Real-World Example
Ransomware	Disables victim's access to data until ransom is paid	**RYUK**
Fileless Malware	Makes changes to files that are native to the OS	Astaroth
Spyware	Collects user activity data without their knowledge	DarkHotel
Adware	Serves unwanted advertisements	Fireball
Trojans	Disguises itself as desirable code	**Emotet**
Worms	Spreads through a network by replicating itself	Stuxnet
Rootkits	Gives hackers remote control of a victim's device	Zacinlo
Keyloggers	Monitors users' keystrokes	Olympic Vision
Bots	Launches a broad flood of attacks	Echobot
Mobile Malware	Infects mobile devices	Triada
Wiper Malware	Erases user data beyond recoverability.	WhisperGate

When you go to some websites, you may see the **green rectangles** shown below, asking you to download a program.

It is recommended not to click on these as they usually aren't part of the program you want to see and may cause trouble for your computer !

Prevent malware

- Install antivirus / malware software.
- Keep your antivirus software up to date.
- Run regularly scheduled antivirus scans.
- Keep your operating system and software up to date.

MALICIOUS MALWARE DISTRIBUTION

Categorized by how they spread

- Worms & Viruses – Self Replicating
- Trojan horse – Disguised as legitimate program
- Malvertising - false/fake advertisement

MALICIOUS SOFTWARE ACTIONS

Categorized by what they do

- Ransomware – Holds files for ransom
- Adware – Pop-up Ads
- Spyware – Hides and steals info
- Botnets and zombies – Used to attack others

RANSOMWARE: A COSTLY DIGITAL THREAT

- **RANSOMWARE IS MALICIOUS SOFTWARE THAT LOCKS YOUR COMPUTER OR ENCRYPTS YOUR FILES, DEMANDING PAYMENT—OFTEN IN CRYPTOCURRENCY—FOR RELEASE.**

- Victims face not only ransom costs but also data loss, downtime, and reputational harm.

- Seniors are especially vulnerable due to limited cybersecurity resources.

5 Key Statistics on Ransomware Losses

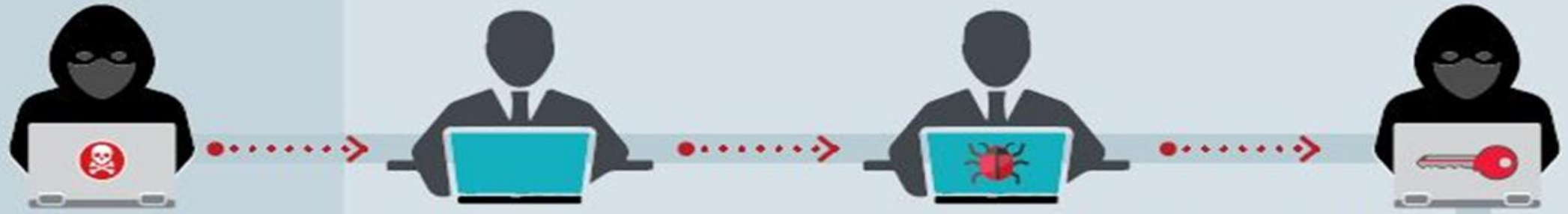
❖ $57 billion - Estimated global cost of ransomware in 2025, including ransom payments, downtime, and recovery.

❖ $2.73 billion - Total ransom demands in 2024, up nearly $1 billion from the previous year.

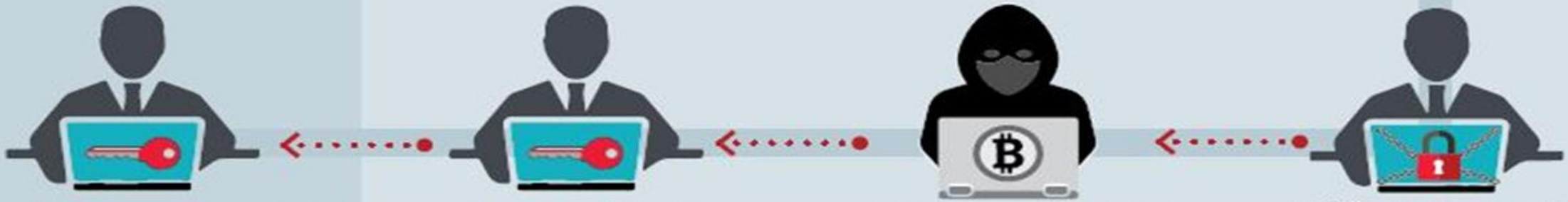
❖ $1.85 million - Average cost per ransomware incident, factoring in business disruption and data restoration.

❖ 80% of victims - Paid the ransom, yet many were attacked again shortly after.60% of organizations.

Anatomy of a ransomware attack



1. Attacker sends a phishing email
2. User receives a link and clicks
3. Malware unpacks and executes
4. Attacker gains control of 'the public key' required to encrypt files



5. Files get encrypted and user gets ransomware screen
6. Attacker demands ransom from user (e.g. Bitcoin)
7. When ransom is paid, attacker may deliver 'the private (decryption) key'
8. Files are decrypted.*

Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

SOCIAL ENGINEERING

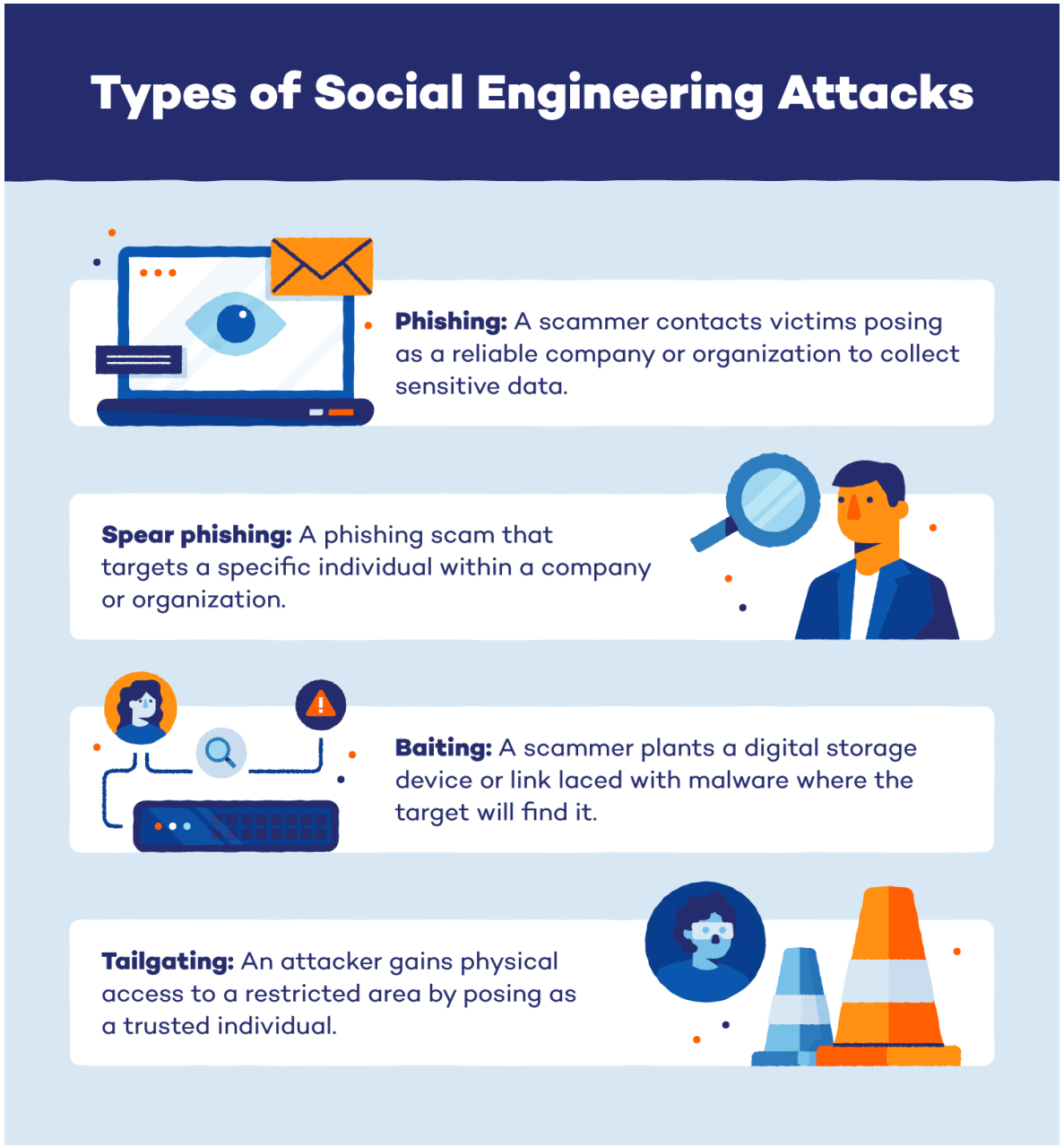
Instead of exploiting technical vulnerabilities, **social engineering preys on human traits such as trust, fear, curiosity, and urgency to persuade victims.**

Often called "human hacking," is a tactic that exploits human psychology to manipulate or deceive people into giving up confidential information or performing actions that compromise their personal or organizational security.

Essentially, it's the art of tricking someone into making a security mistake.

The goal is typically to steal sensitive information like passwords and financial data, or to gain access to a computer system or network.

Phishing is one of the most common forms of social engineering.



Signs of a Social Engineering Attack

- You don't recognize **the sender**
- You receive an **unexpected email**
- Email or ad offers a **free download**
- The request is **urgent**

Avoid Social Engineering Attacks

- Never click on **unfamiliar links**
- Delete **suspicious requests** for sensitive information
- Update your **spam filters**
- Secure your devices with **antivirus software**

PROTECT YOUR INFORMATION !!

- Authentication
- Privacy
- Encryption
- Backups

AUTHENTICATION

First line of defense!
Identify and Prove

Forms of Authentication

- Username and Password
- Finger Print Readers
- Facial Recognition
- Card and Pin

Choose a Password

A password that is easy to remember is easy to hack.

Password examples

Bad	Better	Best
accident	AcciDent	Acc!Den7
smellycat	sm3llycat	$m3llyc@t
creditunion	CreditUnion	Cr#ditUn1on

CREATING A GOOD PASSWORD

THE 25 WORST PASSWORDS TO USE

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars
26. **incorrect**

TIPS FOR CREATING STRONG PASSWORDS

- **Never use personal information** such as your name, birthday, username, or email address. This type of information is often publicly available, which makes it easier for someone to guess your password.

- **Use a longer password**. Your password should be **at least 12 characters long**, although for extra security it should be even longer.

- **Don't use the same password for each account**. If someone discovers your password for one account, all of your other accounts will be vulnerable.

- Try to include **numbers, symbols**, and both **uppercase** and **lowercase letters**.

- Avoid using words that can be **found in the dictionary**. For example, **swimming1** would be a weak password.

You could also consider using: $ for an s, % or a # for a p, the number 0 for an o,@ for an a, etc.

CREATING STRONG PASSWORDS

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	17 mins
7	Instantly	Instantly	2 hours	9 hours	20 hours
8	Instantly	30 mins	5 days	3 weeks	2 months
9	Instantly	13 hours	9 months	4 years	11 years
10	Instantly	2 weeks	40 years	232 years	779 years
11	Instantly	1 year	2k years	14k years	54k years
12	2 hours	26 years	107k years	889k years	3m years
13	1 day	684 years	5m years	55m years	267m years
14	1 weeks	17k years	291m years	3bn years	18bn years
15	3 months	462k years	15bn years	212bn years	1tn years
16	3 years	12m years	788bn years	13tn years	91tn years
17	28 years	312m years	40tn years	815tn years	6qd years
18	276 years	8bn years	2qd years	50qd years	449qd years

The Sun Will Come Out, Tomorrow, Bet Your Bottom Dollar

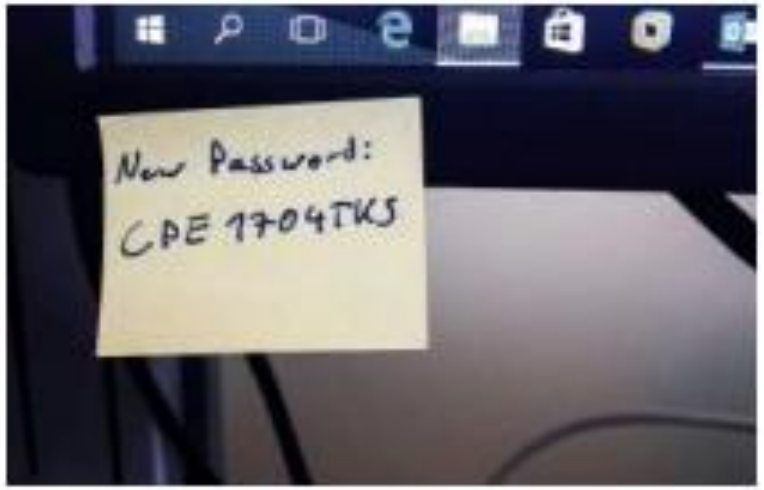
tswcotbybd	Random!
tswco)t(bybd	12 Characters + Symbols!
TsWc0)t(ByBd	Mixed case and numbers!
a$TsWc0)t(ByBd	Add “a$” for Amazon.com
emTsWc0)t(ByBd	Add “em” for email

https://howsecureismypassword.net/

PROTECT YOUR PASSWORD

Always keep your secret to yourself!

- Don't write it down!
  - If you do, keep it in a secure place
- Don't store passwords in programs
  - Browser/Website
  - Save login
- Don't tell anyone for any reason
  - Not to family
  - Not to the IT Guy
  - Not to anyone on the phone
- Change your password from time to time
  - Secure passwords can be compromised
  - Recommended every 90-180 days

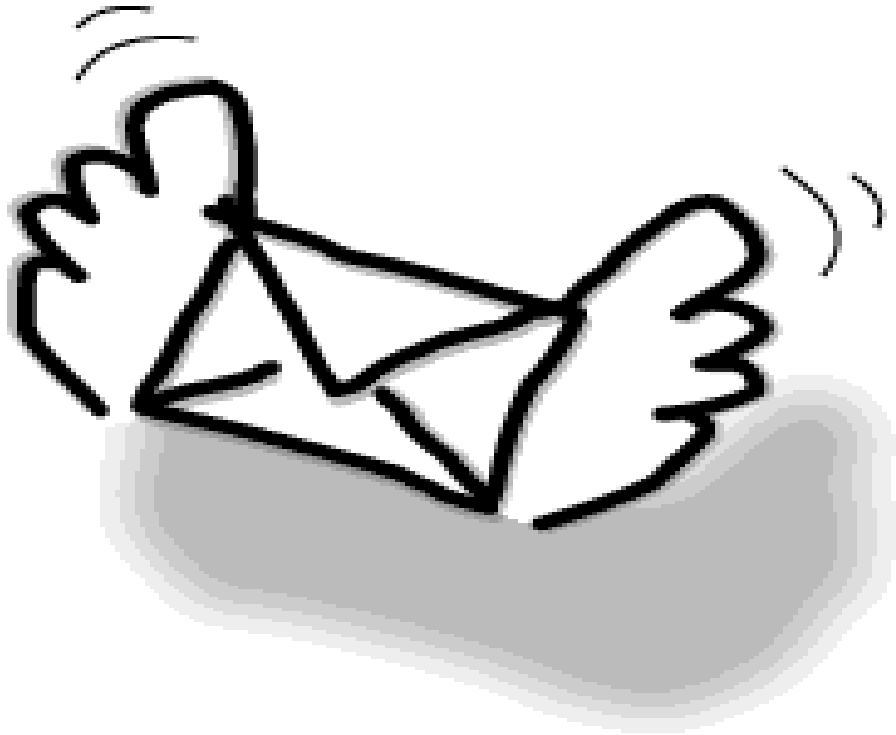


Email and Phishing

Very common and very difficult to identify.

E-MAIL: STAYING IN TOUCH

- **E-mail** is short for electronic mail.
- It’s the most popular of the Internet services.
- Messages are sent and received in a few seconds.
- It’s a modern method of transmitting data, text files, digital photos, and audio and video files, from one computer to another, over the internet.



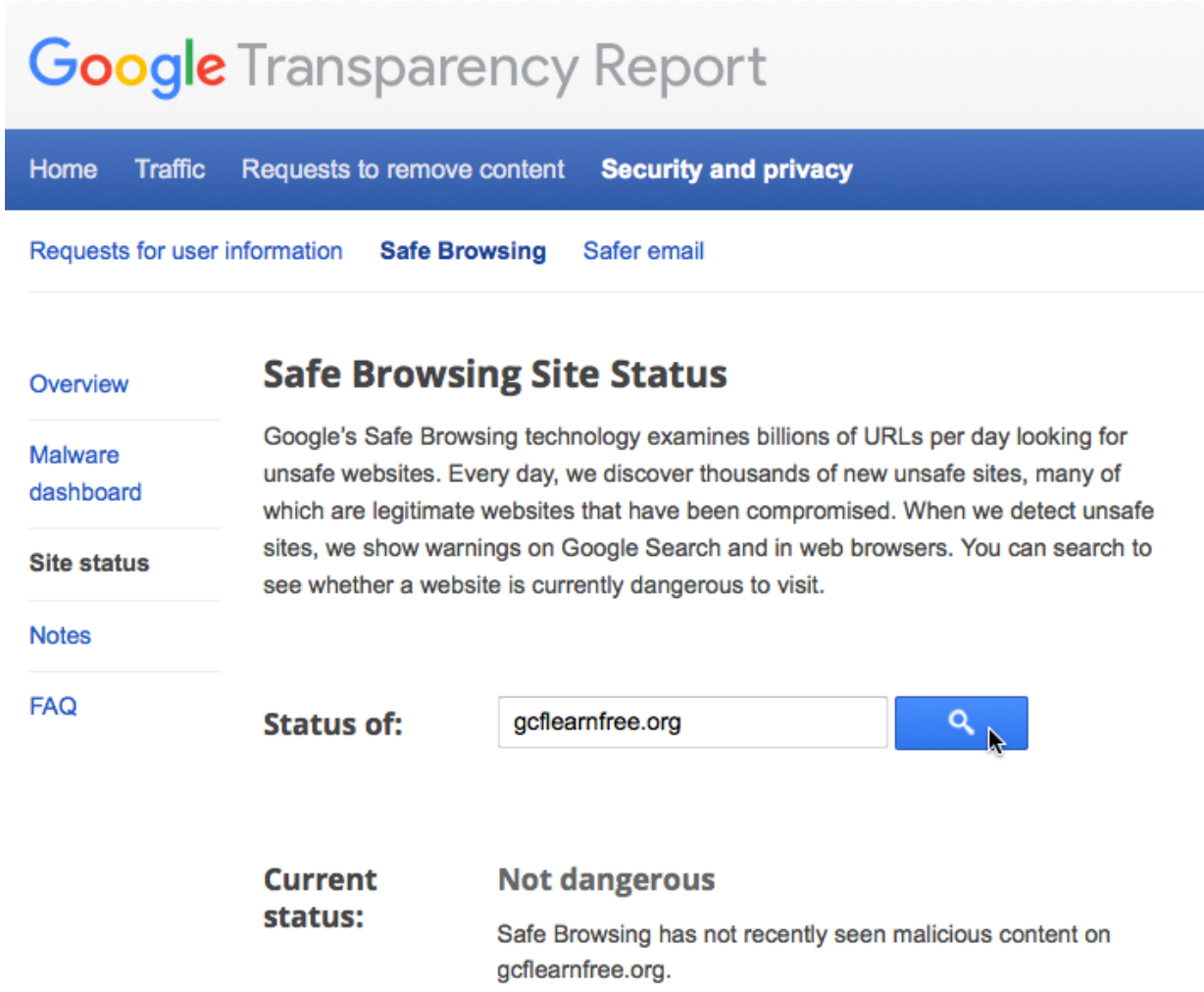
IDENTIFY SUSPICIOUS SITES - If you're ever unsure whether a website or download is safe, close it and investigate the site before returning to it. It's always a good idea to be cautious when browsing unfamiliar sites.

- **Ask your friends** if the site is reputable or if they have any experiences with the site.

- **Search for information about the site**. Use a search engine to find news about the organization that runs the site or look for posts on forums about other people's experiences with that site.

- **Check the address bar in your browser**. Some malicious websites are designed to look like other well-known sites, but your address bar will tell you which site you're actually on. If you are no longer on the site you expected to be, it's suspicious.

- **Run a Google safe browsing diagnostic** on the site. Copy and paste the URL of a site into the search box on the diagnostic page, then click the search button. This will display a site safety report.

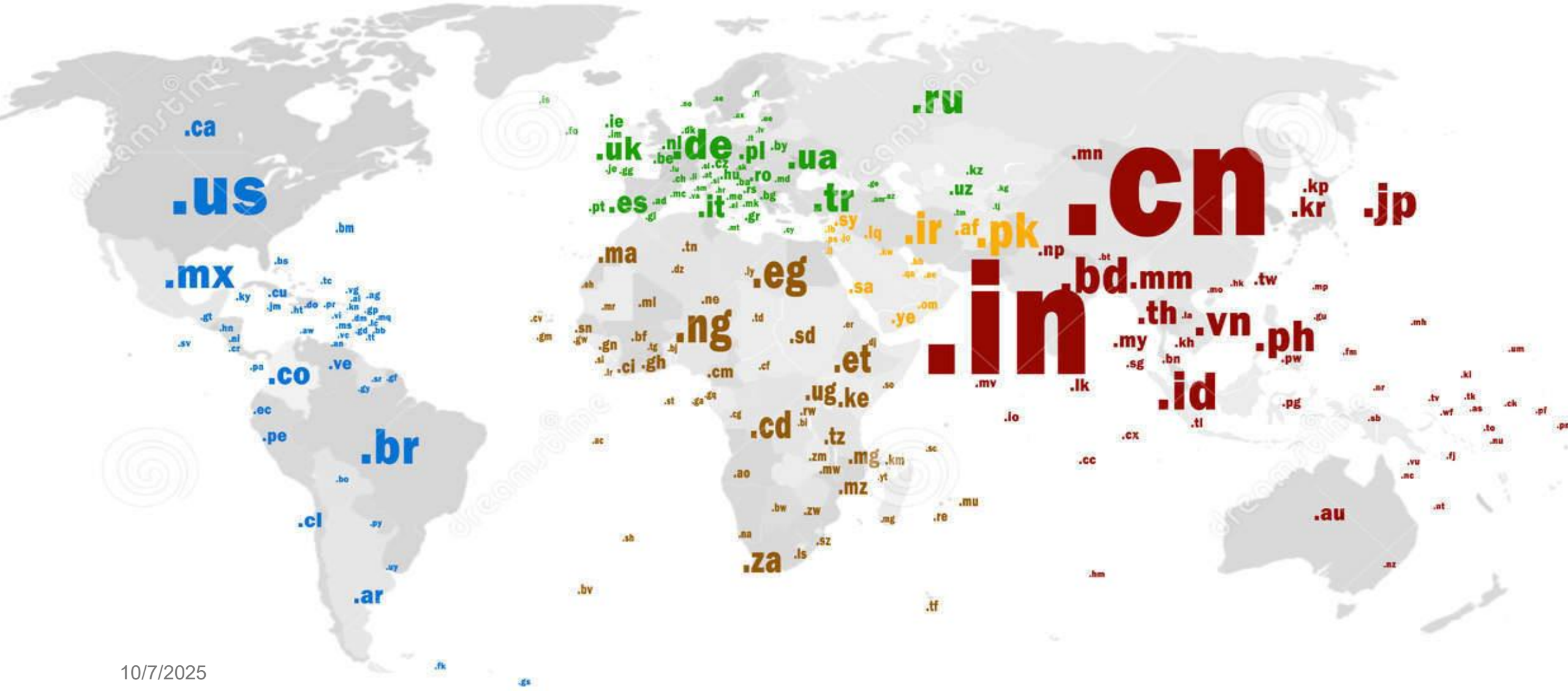


THE COMMON EXTENSIONS FOR DIFFERENT ORGANIZATIONS

.edu	Educational organization (most US universities)
.k12	US school site (not all US schools use this)
.ac	Academic institution (outside of US)
.sch	School site (some schools outside of the US use this)
.com	Company (usually .co in the UK) (future ones may be .biz)
.org	Any non-profit organization
.gov	Government agency
.net	Network
.mil	Military institution

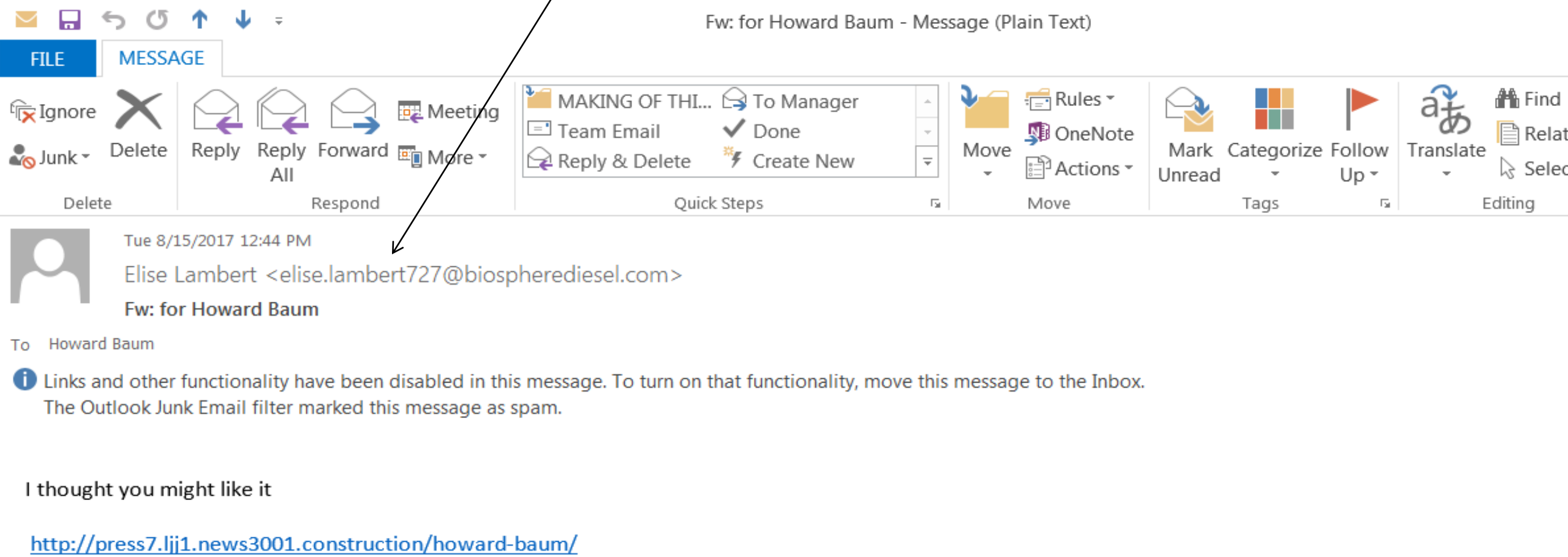
Extensions can also include country codes, such as .uk, .ca, .za, br, etc.

For sending e-mail messages to places outside of the United States, to a friend who lives in Brazil, I would type out their whole e-mail address and follow it with .br



This is a good example of a phishing or Spam message.

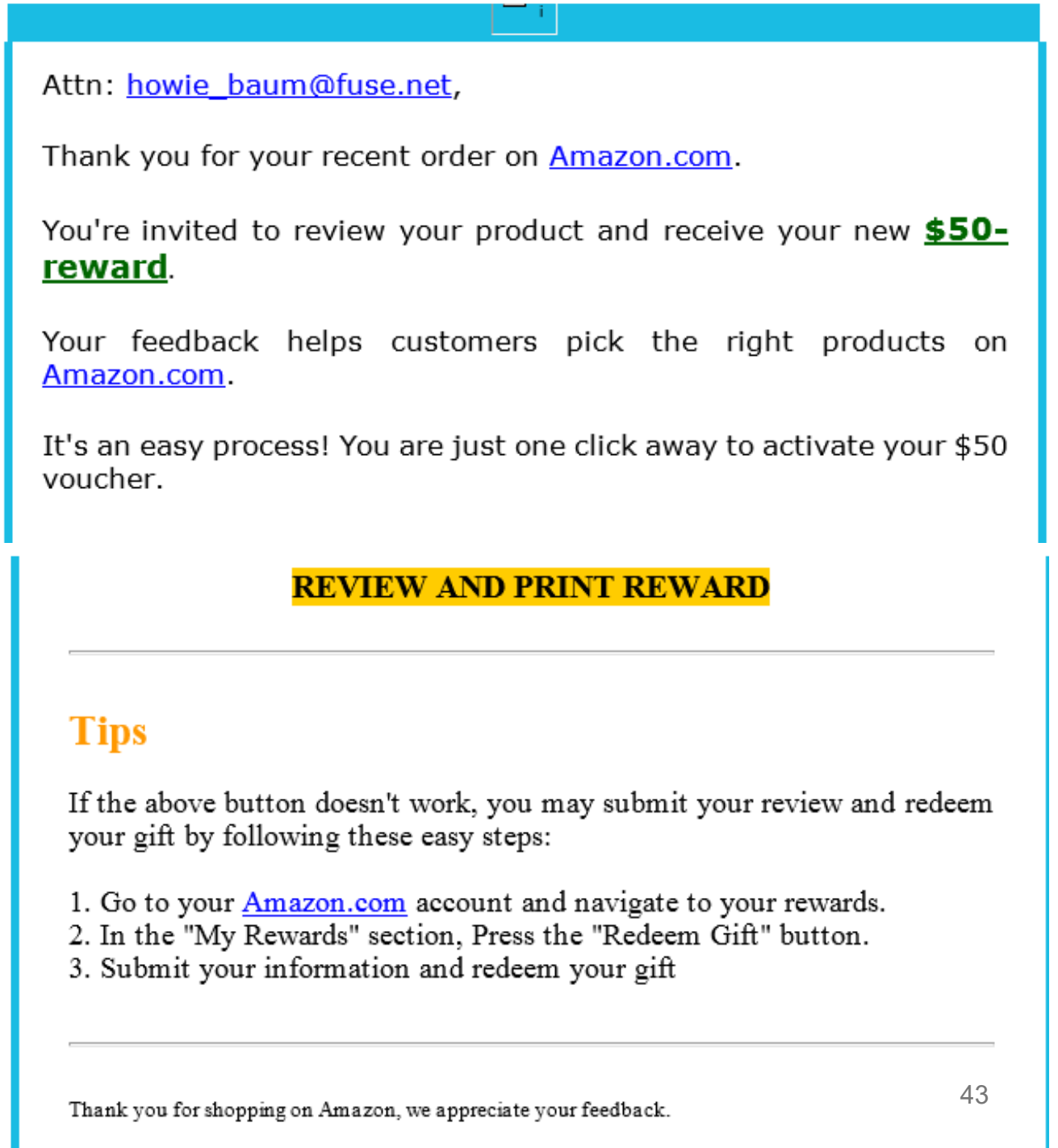
It looks like its from my Daughter Elise but her e-mail address isn't the same as the one she uses all of the time. Its important to look at and check the e-mail address to be sure its from someone you know or a reliable website.



This is another example of a Phishing message that I received twice, at home. It offered me a $50.00 reward at Amazon if I would click on a link.

The only thing that I bought a few months ago from Amazon, cost $40.00 so this is one of those messages that sounds “TOO GOOD TO BE TRUE” !

I checked the actual e-mail address it was from and it wasn’t an authentic Amazon address so then my belief was confirmed.



Attn: howie_baum@fuse.net,

Thank you for your recent order on Amazon.com.

You're invited to review your product and receive your new **$50-reward**.

Your feedback helps customers pick the right products on Amazon.com.

It's an easy process! You are just one click away to activate your $50 voucher.

REVIEW AND PRINT REWARD

Tips

If the above button doesn't work, you may submit your review and redeem your gift by following these easy steps:

1. Go to your Amazon.com account and navigate to your rewards.
2. In the "My Rewards" section, Press the "Redeem Gift" button.
3. Submit your information and redeem your gift

Thank you for shopping on Amazon, we appreciate your feedback.

This a good example of a real Phishing e-mail message. I have an account set up with Cincinnati Bell for use of my computer, a home phone, and cable for TV.

Watch out when a company you use, asks for any personal or computer information or to click on a link, like below, as its not something they normally do. **Important:** Always look at how their e-mail address reads.

The one below says little about being from Cincinnati Bell (just on the last line) and the last 2 digits says its from Brazil so I made sure to permanently delete it, right away !!

Helpdesk,

CB Cincinnati Bell Support, <lorenzo.souza@pm.es.gov.br>
To

Reply | Reply All | Forward | ...

Sun 4/11/2021 4:56 AM

Dear Subscriber,

This message is from Cincinnati Bell Technical Support Help Desk,
We are currently upgrading our fuse.net e-mail database and e-mail account center i.e., homepage view, enhance security installations of new 2021 anti-spam and anti-virus software, we are deactivating old email users to create more space for our email database.

We appreciate your support in protecting your data. Kindly verify your fuse.net e-mail within 24 hours or your e-mail will be deactivated. Click Here to verify your e-mail.

Thanks for your co-operation,

Fuse.Net IT HelpDesk,
Fuse.Net Support Help Desk,
© 2021 Cincinnati Bell Inc,

Two-Factor Authentication

Why aren't passwords good enough?

MULTIFACTOR AUTHENTICATION

Using two or more methods to authenticate

Something you have

- Smartphone
  - Text, App, Phone call
- Smart card, ID card, Credit Card

Something you know

- Password
- PIN Number
- Passphrase

Something you are

- Fingerprint
- Facial Recognition
- Eye Scan

PERSONAL INFORMATION ONLINE

YOUR PII CHART™

Take time to inventory the identity relationships you have with the companies, organizations, and individuals you entrust with your personally identifiable information or PII. See how your identity is a PII Chart™, a picture of relationships you've created. Once you visualize the slices of your PII, managing your identity assets becomes easier.

LEGEND

- **SOCIAL SECURITY NUMBER**
- **CONTACT INFORMATION** (email address, physical address, telephone and mobile numbers)
- **GOVERNMENT-ISSUED IDENTIFICATION** (driver's license, passport, birth certificate, library card)
- **BIRTH DATE, BIRTH PLACE**
- **ONLINE INFORMATION** (Facebook, social media, passwords, PINs)
- **GEOLOCATION** (smartphone, GPS, camera)
- **VERIFICATION DATA** (mother's maiden name, pets' and kids' names, high school, passwords)
- **MEDICAL RECORDS INFORMATION** (prescriptions, medical records, exams, images)
- **ACCOUNT NUMBERS** (bank, insurance, investments, credit cards)

PROTECT YOUR IDENTITY

- Don’t give out personal information when asked
- Read your credit card and bank statements
- Bring in your mail everyday
- Use a paper shredder
- Freeze your credit or use credit monitoring services
- Set up alerts
- Follow all the other tips in this seminar

TYPE	DEFINITION
Financial Identity Theft	Involves Theft of a Victim's Financial Information for Fraudulent Purchases or Obtaining Credit
Criminal Identity Theft	Involves Use of a Victim's Personal Information During an Arrest or Investigation
Medical Identity Theft	Involves Using a Victim's Information to Get Medical Care, Drugs, or Insurance Benefits
Tax Identity Theft	Involves Filing a Fraudulent Tax Return in the Victim's Name to Obtain a Refund
Child Identity Theft	Involves Unauthorized Use of a Minor's Personal Information for Fraudulent Purposes
Synthetic Identity Theft	Involves Creating a Fake Identity With Real and False Information, Often Using Stolen Social Security Numbers
Employment Identity Theft	Involves Using Someone Else's Information to Obtain Employment to Work Illegally or Evade Taxes

Identity Theft Prevention Strategies for Individuals

- **Secure Personal Information**
- **Protect Your Social Security Number**
- **Monitor Financial and Personal Accounts**
- **Be Vigilant With Mail and Personal Documents**
- **Be Cautious Online**
- **Use Two-Factor Authentication**

PRIVACY ONLINE

Social Media

- Use privacy settings and security settings
- Be careful what you share
- Understand the terms and conditions

Cookies (Web tracking)

- Deleting cookies
- Use private browsing modes

Location Services

- Choose which apps or website can use your location
- Disable Location Services completely

DATA PROTECTION - BACKUPS

3-2-1 Rule

3 Copies of your data

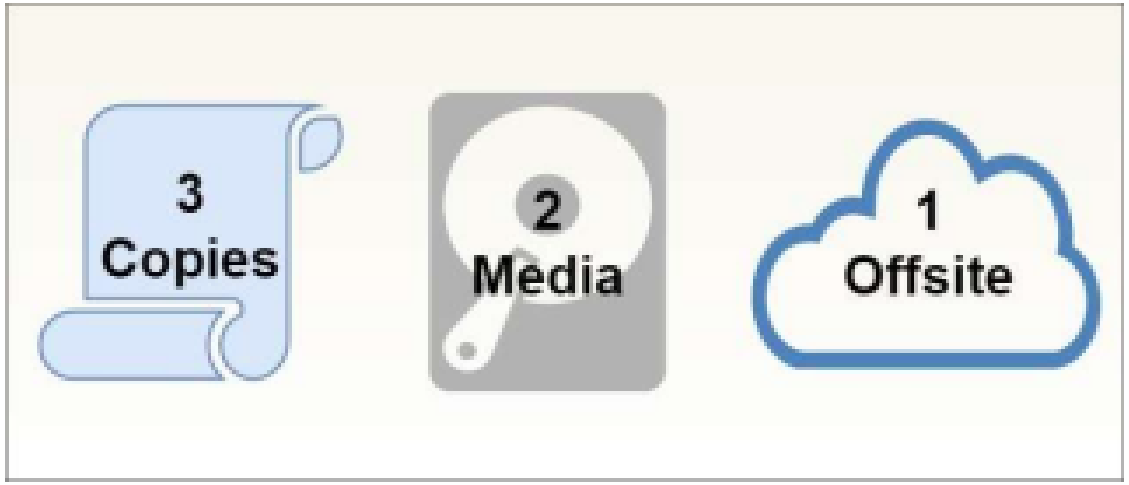
One Primary Copy and Two Backups

2 Types of Media

Hard Drive, File Server, Cloud

1 Off-Site Storage

Cloud



Backup Methods
Manual Backup
Scheduled Automated Backup
Sync Backup

DATA PROTECTION – BACKUP METHODS

Manual Backup
- Copy Important Files to External Storage

Scheduled Automated Backup
- Built in Tools for Windows or Apple OSX
- 3rd Party Tools

Sync Backup
- Desktop Sync Services
  - Google Drive
  - Microsoft One Drive
  - Apple iCloud

- Phone Sync Services
  - Google Sync
  - iOS Backup
  - 3rd Party

PROTECTING YOUR DEVICES

- Updates
- Antivirus
- User Permissions
- Mobile Devices

It All works with the Cloud !!


SORRY, BUT THIS IS NOT WHERE YOUR COMPUTER INFORMATION IS STORED

INTERNET DATA CENTERS – THIS IS THE CLOUD !!

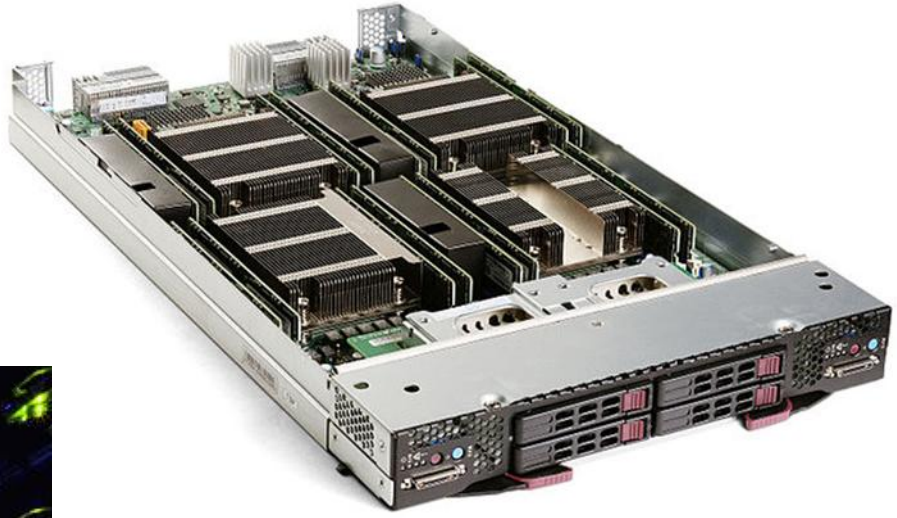
As of September, 2025, the United States had 5,400 data centers, which is more than any other country in the world.

They provide the newest computer storage and calculating resources for over 19,662 service providers such as all the Cloud sites, Spectrum, AltaFiber, Dish Network, etc.

This data center handles 3 million websites all the time.

Part of the CBS Sunday Morning show – A Visit into the “Cloud” which is 8.3 minutes long and this segment goes from 3.11 min to 4.37 min (1.5 min)
https://www.youtube.com/watch?v=94PO2-TL4Vs

The average full-scale data center is 100,000 square feet in size and runs around 100,000 servers, which are essentially powerful computers.



A HIGH-SPEED COMPUTER SERVER

TYPES OF SCAMS

DATING & ROMANCE

Scammer uses fake profiles to lure you into a relationship, then asks for money or you to invest in something

INVESTMENT

Fake investment opportunities used by scammers to get you to hand over your money

BUYING OR SELLING

Fake online stores or classified ads to sell you a product or service that doesn't exist

REMOTE ACCESS

You are asked to hand over control of your device to fix a problem. Scammers may pretend to be from your local council, electricity or gas company, or internet/ phone provider.

FAKE CHARITIES

Often occurring after natural disasters or other major events, the scammer mimics genuine charities in an attempt to get your money and private information

PHISHING

Sending emails or other messages pretending to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

TRAVEL, PRIZE & LOTTERIES

Tricks you into handing over personal information for you to receive a 'free' prize from a competition or lottery you never entered

JOBS & EMPLOYMENT

The promise of a high-paying job that doesn't exist where you are asked to pay for your training. Also includes Ponzi or Pyramid Schemes

SOFTWARE UPDATES

Why are Updates Important?

- Fix Security Vulnerabilities
- Fix Bugs or unexpected errors
- May include enhancements or new features

Are there downsides to updating?

- Your device may need to be restarted
  - Make sure to save your work
- Updates can be slow
  - Doing them regularly reducing the time
- Don't power down your device until updates complete
  - Can cause the things to break

WHAT TO UPDATE

Operating System
- Windows
- Mac OSX
- iPhone –iOS
- Android

Applications
- Microsoft Office
- Adobe
- Java
- Phone Apps

Connected Hardware (Firmware)
- Printers
- Web Cams
- Keyboard/Mouse
- Digital Camera
- External Drives

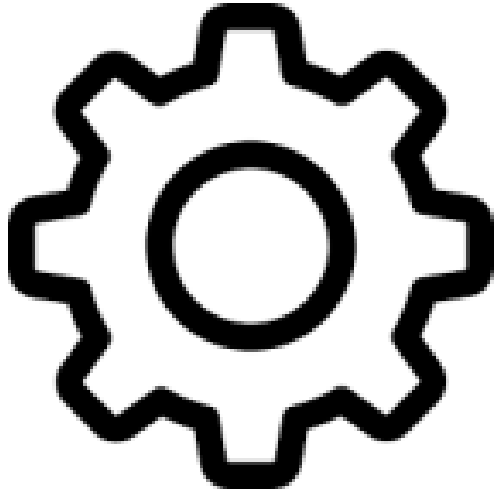
WHEN AND HOW TO UPDATE

Update Often

- Most updates released monthly
- Important security updates released ASAP
- Setup Automatic Updates
- Make sure you are using the latest versions

Use Settings Menus to Configure Updates

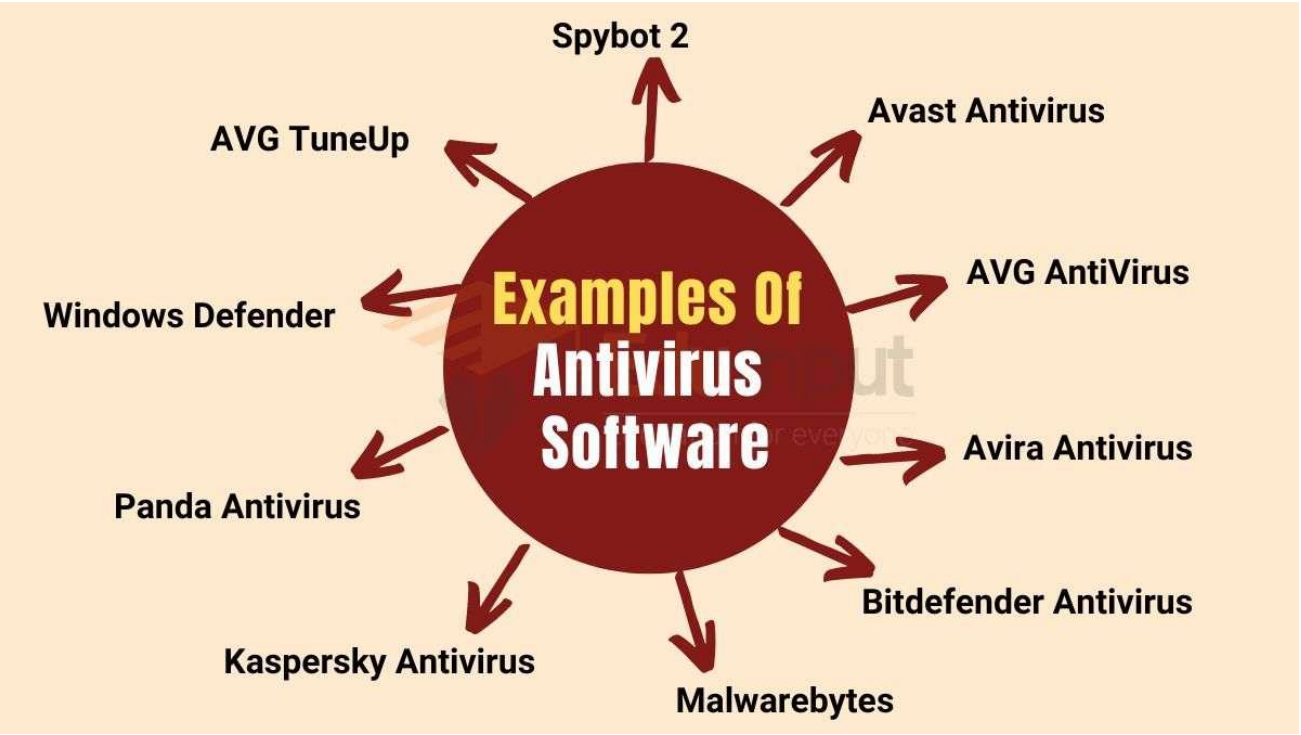
- Windows
- Mac OSX
- iOS
- Android



Download Manufacture Software for Devices

Logitech
Dell
HP

ANTIVUS: WHAT TYPE IS BEST ?



Free

- Windows Defender
- Malware Bytes
- AVG Free

Paid

- Norton Security
- McAfee
- Bitdefender
- Kaspersky

Internet Service Provider Options

- Cincinnati Bell (now Altafiber)
- Spectrum
- Comcast
- AT&T

ANTI-VIRUS – I DON'T USE WINDOWS

Yes! Apple MacOSX can get viruses

Yes! Smartphones can get viruses

Yes! Linux can get viruses

Yes! Any computing device could get a virus

Microsoft devices use Windows Defender

Apple devices use 4 background malware protection programs that update regularly..

- Xprotect
- Gate Keeper
- Notarization
- System Integrity Protection (SIP)

LOCAL USER ACCOUNTS

Why use different accounts

- Enforce password usage
- Manage security for each person
- Using standard account can prevent malicious software
- Creates isolated workspace for each person
- Set up parental controls (Windows)
- Allow guests safe access to computer

PROTECTING MOBILE DEVICES

- **Lock your phone**
  - Setup passcode, pattern, fingerprint, etc
- **Setup auto lock features**
  - Less than a minute is ideal
- **Check app permission when downloading**
  - Does the app need to access you contact lists?
- **Avoid public charging stations**
  - Carry a spare charging device
- **Avoid public Wi-Fi**
  - If you must, use a VPN
- **Install Anti-virus**
- **Turn off location services if not needed**
- **Never leave unattended**

Common ways a cybercriminal can hack your phone

HOME NETWORKS – WI-FI (WIRELESS)

Wireless Router/Access Point

- Connects all your devices together and to the Internet
- First line of defense into your home network

Wireless Router Security

- Change default passwords
  - Admin password and Wi-Fi Password
- Use Guest network
  - Don't share you main Wi-Fi password
- Use Wireless Network Encryption

- Keep router to date
  - Software
  - Replace hardware that is more than 10 years old
- Keep firewall on

PUBLIC NETWORKS – WI-FI

Connecting to public Wi-Fi can be dangerous

- Avoid if possible
  - Use a personal hotspot/phone
- Don't shop, access your bank, or other sensitive activity
  - Someone could be watching
- Never use open networks
  - No password
  - Definitely a bad network
- Look out for rouge networks
  - Verify network name and password
- Turn off automatic connectivity feature
- Use a VPN (Virtual Private Network)

IDENTIFYING A PHISHING ATTACK

Message my look legitimate, but look out for…

- **A message that makes you PANIC!**
- **A message that asks for sensitive information**
- **A message that asks you to do something out of the ordinary**
- **A message that offers you money**

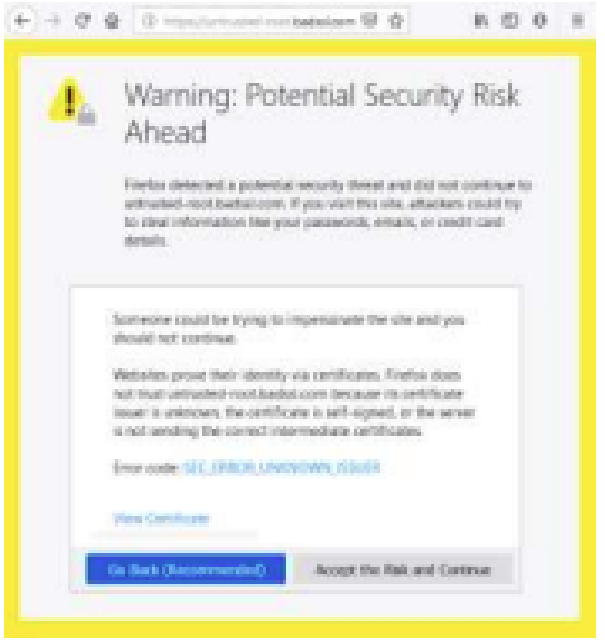
Red Flags!

- Typos or bad grammar
- Strange e-mail or web address
- Links or attachments

IDENTIFYING MALICOUS WEBSITES

A website may be malicious if....

- It prompts you to download a file or run a program
- It says you are already infected with malware
- It says your browser is out of date
- Tells you won a prize
- Offers free software



Look out for other red flags

- Check the URL for misspellings
- No contact info
- Too good to be true
- No encryption/certificate

IDENTIFYING PHYSICAL ATTACKS

Not all attacks start from a computer

- Dumpster Diving
- Skimmers
- USB Drops
- IoT (Internet of Things)

DISINFORMATION

Spotting "Fake News"

Types

- Deliberate Misinformation
- Fales Headlines "Clickbait"
- Social Media Sharing
- Satire

Consider the source

- Look at the URL
- Be wary of sloppy writing
- Is there supporting information/quotes?
- Are there other sites reporting the story?
- Check against media literacy sites

Consider the motivation

- Is it opinion or reporting?
- Is it prompting a product or person?
- Are sources being paid?

CLICKBAIT

Clickbait is a text or a thumbnail link that is designed to attract attention and to entice users to follow that link and view, read, stream or listen to the linked piece of online content

The image is typically deceptive, sensationalized, or otherwise misleading.

A "teaser" aims to exploit the "curiosity gap", providing just enough information to make readers of news websites curious, but not enough to satisfy their curiosity without clicking through to the linked content. [Wikipedia]

Avoid clicking on them because they might have a virus in them.

Leading Doctor Reveals the No. 1 Worst Carb You Are Eating

Mediconews

The $$$ Moneymaking Secret that Banks Don't Want You To Know

Bankfacts

These 12 Impossible Pet Rescue Stories Will Melt Your Heart!

Cutepups Inc

Safely Install Software

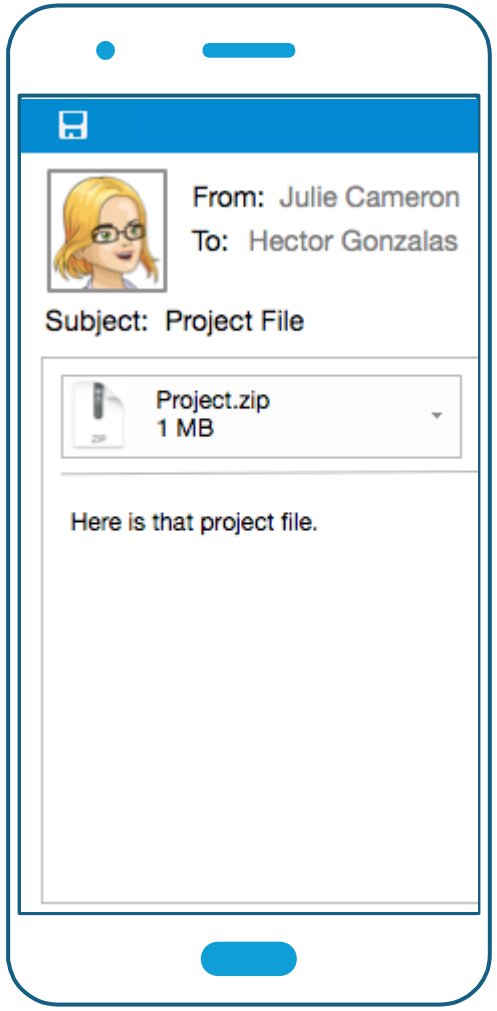
Make sure you're only installing the software you think you're installing.

Install Software the Safe Way

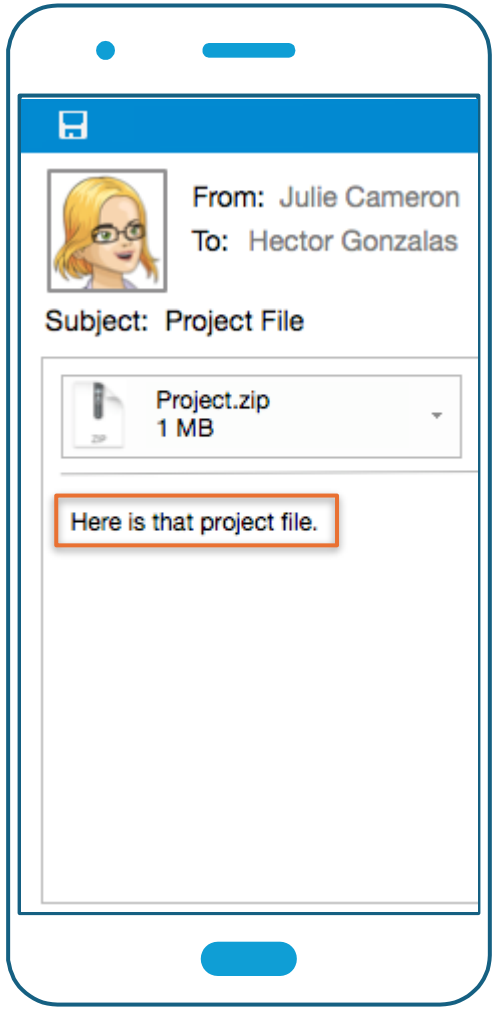
- Don't install personal software on company computers.
- Have up-to-date antivirus software.
- Make sure the software comes from a reliable source.
- Be careful when you install new software; decline any additional software you don't want.

Phishing

Fake emails or websites used to trick people into revealing confidential information.


From: Julie Cameron
To: Hector Gonzalas
Subject: Project File
Project.zip
1 MB
Here is that project file.

Real or Fake?

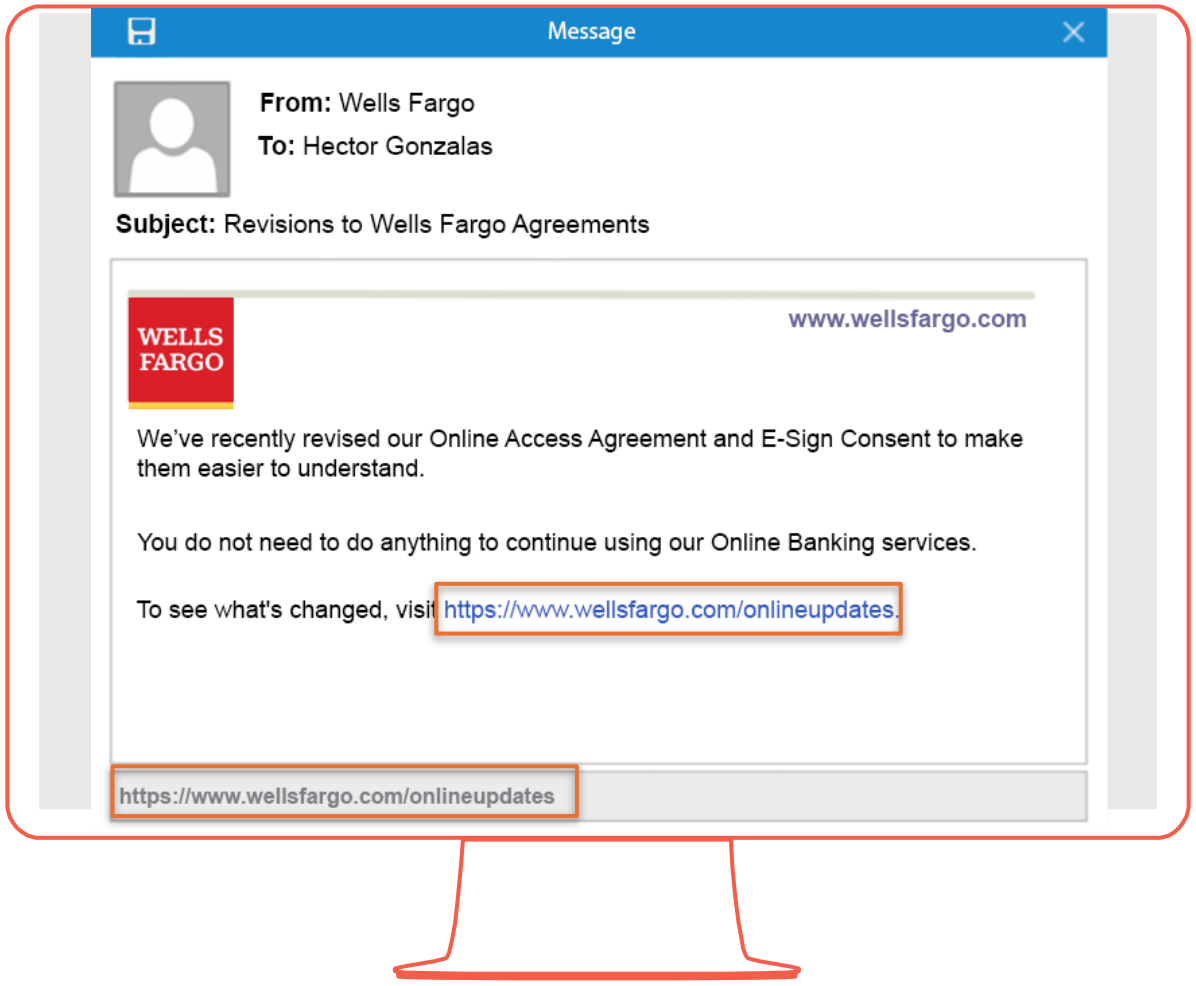


Fake

Emails can appear to come from someone you know; but notice the vague message.

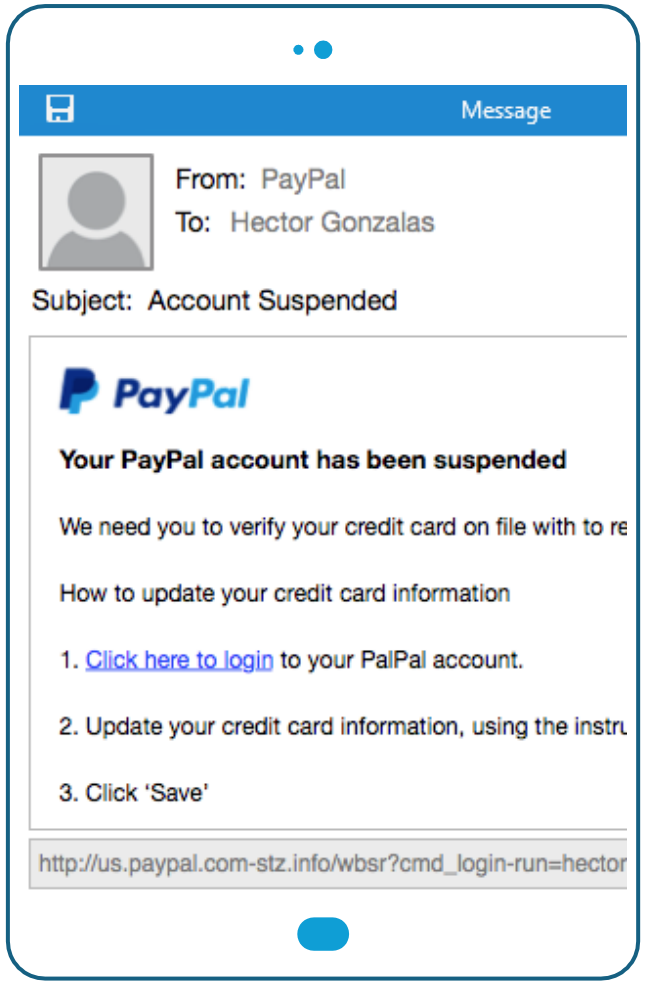

Message
From: Wells Fargo
To: Hector Gonzalas
Subject: Revisions to Wells Fargo Agreements
www.wellsfargo.com
WELLS FARGO
We've recently revised our Online Access Agreement and E-Sign Consent to make them easier to understand.
You do not need to do anything to continue using our Online Banking services.
To see what's changed, visit https://www.wellsfargo.com/onlineupdates.
https://www.wellsfargo.com/onlineupdates

Real or Fake?

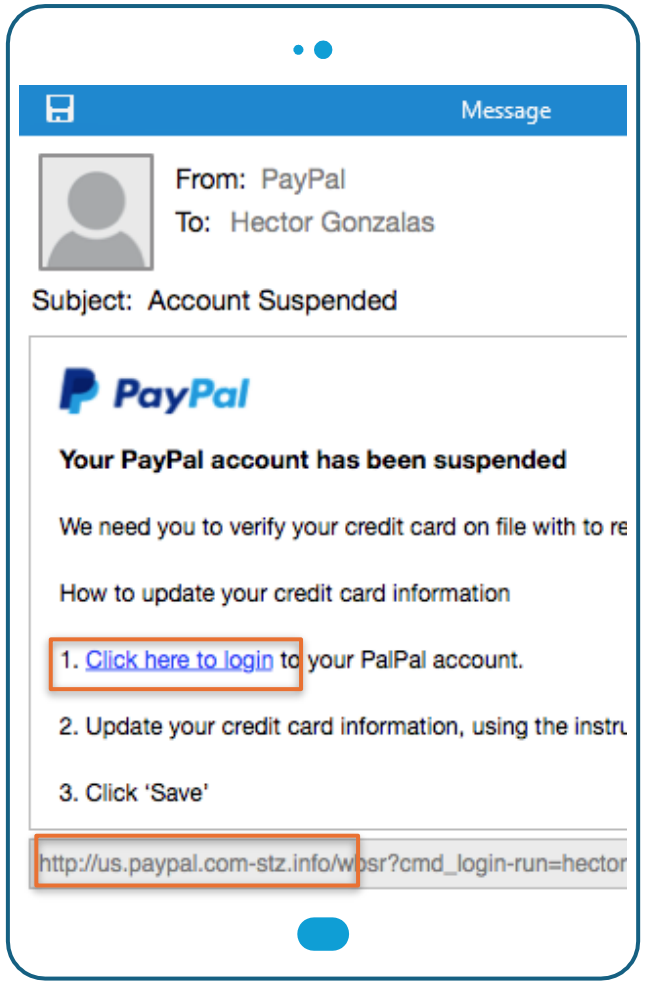


Real

Email is just informational, it's not asking you to do anything.
URL matches what's shown in the link.


Message
From: PayPal
To: Hector Gonzalas
Subject: Account Suspended
PayPal
Your PayPal account has been suspended
We need you to verify your credit card on file with to re
How to update your credit card information
1. Click here to login to your PalPal account.
2. Update your credit card information, using the instru
3. Click 'Save'
http://us.paypal.com-stz.info/wbsr?cmd_login-run=hector

Real or Fake?



FAKE

Link destination is not the official PayPal site.
Emails will usually not solicit you to change your password or login.

Email Security Tips

- Beware of phishing scams / fake emails.
- Unsolicited, legitimate emails will almost never ask you to login.
- Never open attachments in unsolicited or suspicious emails.

Social Media

Quick tips for staying safe.

Be careful what you post to social media

Keep personal information personal.

Social Media Safety Tips

- Adjust your privacy settings.
- Know and manage your friends.
- Keep personal information personal.
- Be mindful of your online reputation.

Protect Your Computer's Data

How to keep your information safe, before a disaster.

Imagine Your Computer is Stolen !

What could someone take from you if that happened?

A Lost or Stolen Computer Gives Someone Access To:

- The computer
- Credentials to log into all your sites
- Information about your financial accounts
- Email and message history
- Files and projects you've worked on
- **RECOMMENDATION: Before anything happens to your computer, back up all of your inforation into a cloud account !!**

TABLE OF COMMON CYBERSECURITY SCAMS

SCAM NAME	METHOD OF CONTACT	DESCRIPTION
Phishing	Email	Tricks user to click link or provide login details.
Smishing	Text Message (SMS)	Deceptive texts with malicious links or urgent requests.
Vishing	Voice Call / Voicemail	Impersonator calls to demand money or sensitive data.
Tech Support Scam	Phone or Pop-up	Fake warning that computer is infected; demands payment and remote access.
Ransomware	Malicious File/Link	Locks files and demands ransom to restore access.
Pretexting	Email/Phone (Targeted)	Uses a convincing fake story to extract specific information.
Romance Scam	Dating Apps / Social Media	Builds a fake relationship, then asks for money for "emergencies.“
Advance-Fee Scam	Email/Letter	Promises large reward after a small, required upfront fee is paid.

QUICK-START ONLINE SAFETY GUIDE FOR SENIORS

1. The Golden Rule: STOP, LOOK, and VERIFY

Never act immediately on an urgent message. Scammers use fear and urgency to rush you.

STOP: If a call, text, or email pressures you, do not respond right away.
LOOK: Hang up or close the message. Take a deep breath.
VERIFY: Call the company or person back using a **known, official phone number** (from a bill or a search, not the number the caller gave you).

2. Three Absolute Scam Red Flags

If someone asks for any of these, it is **always a scam.** End the conversation immediately.

A. **Payment by Gift Card or Wire Transfer.** (No real company or government agency will ever demand this).

B. **Requests for Your Password or Verification Code.** (Never share these).

C. **Unsolicited Request for Remote Computer Access.** (Do not let strangers take control of your device)

D. **Protect Your Digital Doors -** These simple steps stop most online attacks before they start.

3) **DON'T CLICK:** Never click on a link or open an attachment in a strange or unexpected email or text message. Delete it.

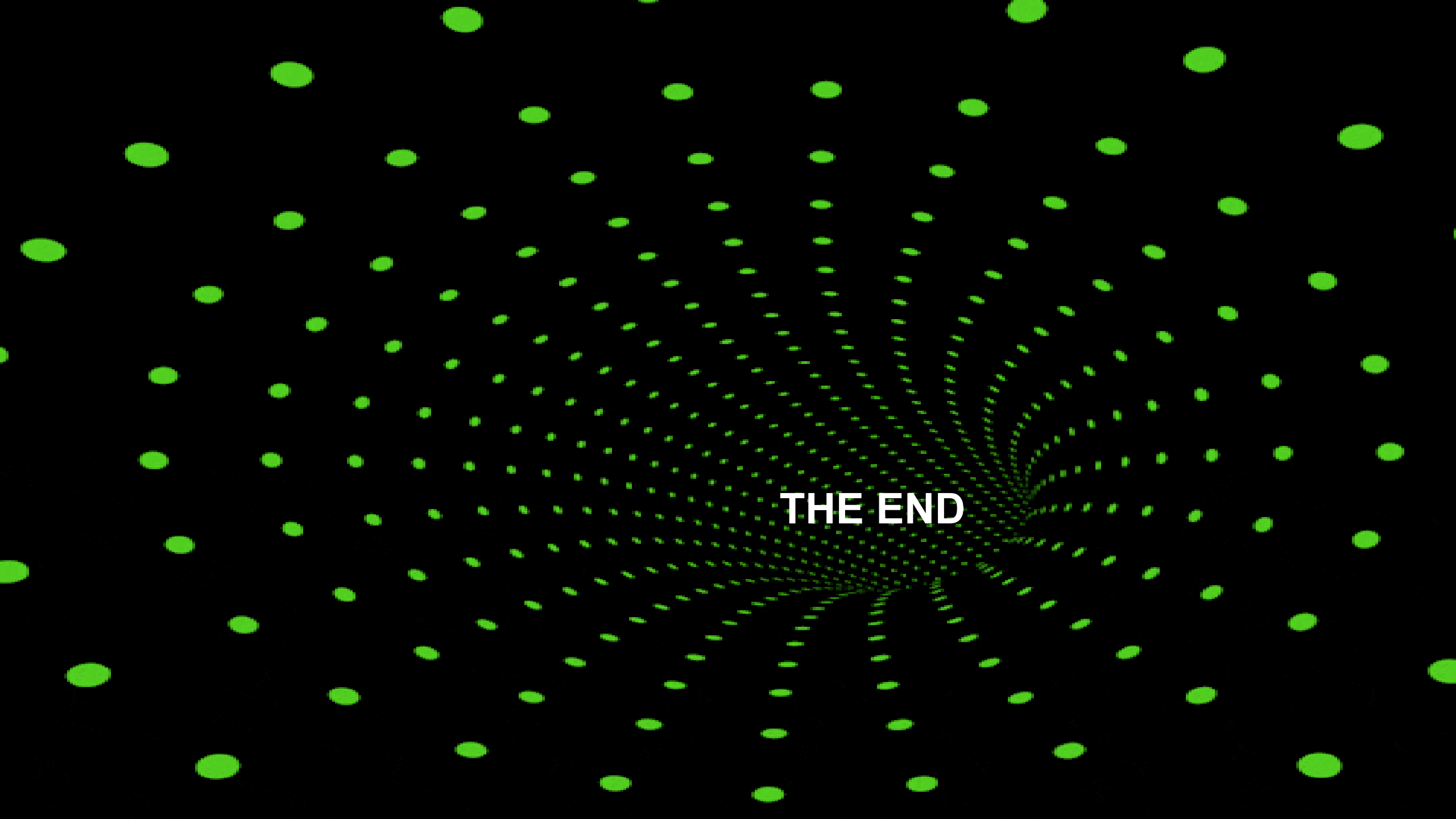
4) **USE STRONG PASSWORDS:** Make every password long, unique, and different for each account. Use a separate, strong password for your email and bank accounts.

5) **ENABLE MFA:** Turn on **Multi-Factor Authentication** (MFA) on your email, banking, and social media accounts. This requires a code from your phone to log in, adding a powerful second layer of security.

6) **KEEP EVERYTHING UPDATED:** Always allow your computer, phone, and apps to install security updates as soon as they are available.

7) **When you answer the phone and there is an unknown caller on the line, NEVER SAY YES !!**

8) **Choose a special word (s) that only your family knows and tell everyone what it is, in case you get an emergency asking for money, ask for the passord to know if it's a real call or not.**


THE END

BIBLIOGRAPHY

OLLI Handouts page: https://ccps.uc.edu/academics/olli/resources/handouts.html

Ohio Cyber Range Institute - https://www.ohiocyberrangeinstitute.org/

https://www.komando.com

howie_baum@fuse.net

https://icscomplete.com/cybersecurity/understanding-different-types-of-malware/

https://www.pandasecurity.com/en/mediacenter/types-of-malware/

https://www.kaspersky.com/resource-center/threats/types-of-malware

https://www.staysafeonline.org/articles/stay-safe-online-related-links

50 Internet Safety tips for 2025 - https://banzai.org/wellness/resources/internet-safety-tips

https://www.malwarebytes.com/cybersecurity/basics/internet-safety-tips

https://cybersecurityforme.com/internet-safety-tips-to-stay-secure-online/

https://iaisp.org/10-internet-safety-tips-cybersecurity-101/

https://www.aarp.org/money/scams-fraud/glossary-of-scam-terminology/ (a good glossary)