



SECURECYBER™

Proven. Proactive. Personalized.

Cybersecurity Awareness

Shawn Waldman - N8VHC

17 July 2025



Introduction

Why are we here today?

- To guide, protect and defend in the daunting world of cyber warfare
- Provide the latest updates on the threat landscape
- Foster cybersecurity-minded culture
- To empower YOU
 - To protect both you and the organization you work for



Security & Safety

- **Security:** We must protect our computers and data in the same way that we secure the doors to our homes.
- **Safety:** We must behave in ways that protect us against risks and threats that come with technology.



Importance of Cybersecurity

- The Internet allows threat actors to attack from anywhere on the planet
- Risks caused by poor security knowledge and practice include:
 - Identity Theft
 - Monetary Theft
 - Legal Ramifications (for yourself and companies)
 - Termination if company policies are not followed
- Top Vulnerabilities
 - Email, Ransomware, Not Patching

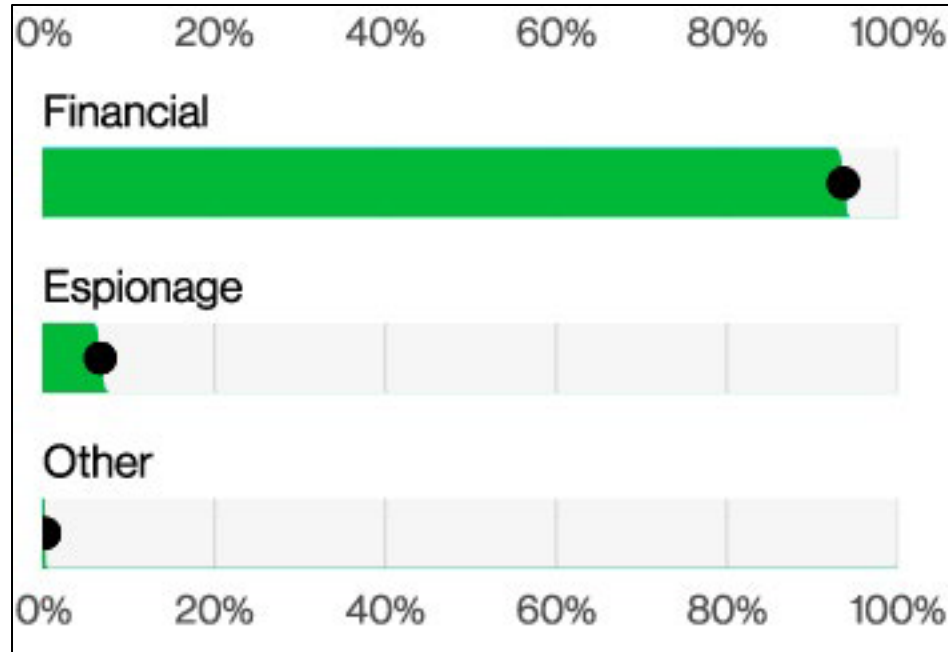




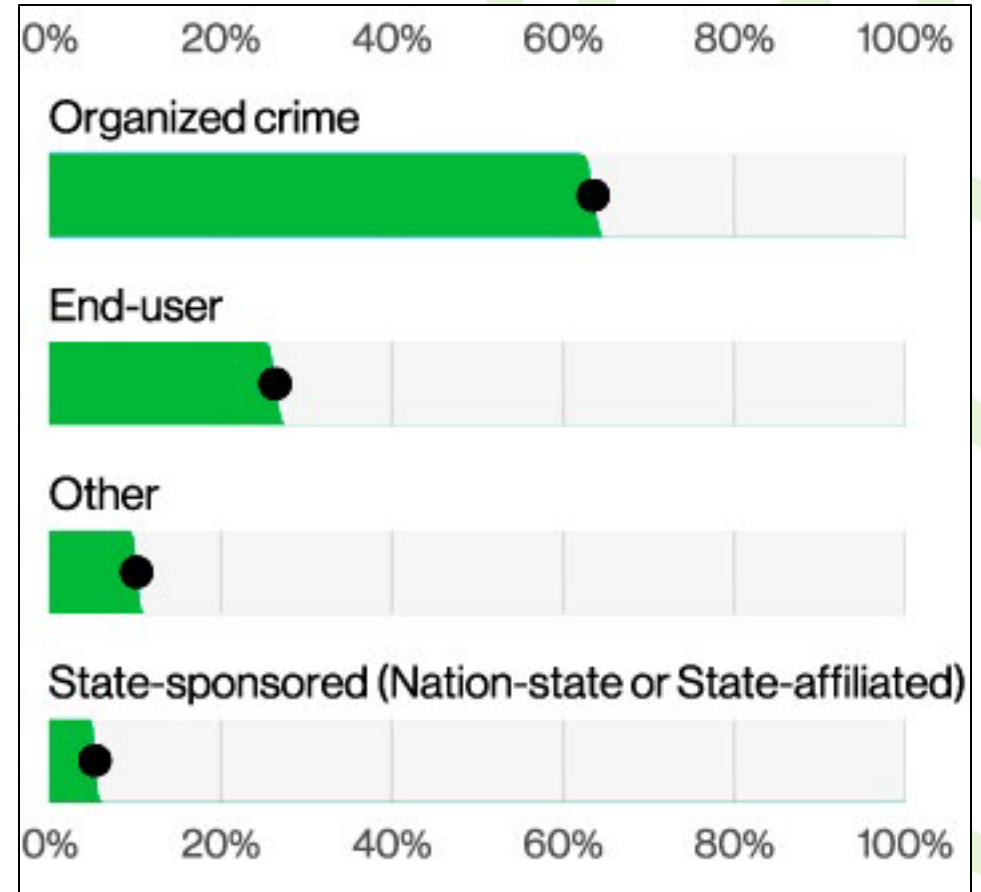
Cybersecurity By the Numbers

Motives & Threat Actors

- Motives



- Threat Actors



2024 Data Breach Investigation Report (DBIR) | Verizon



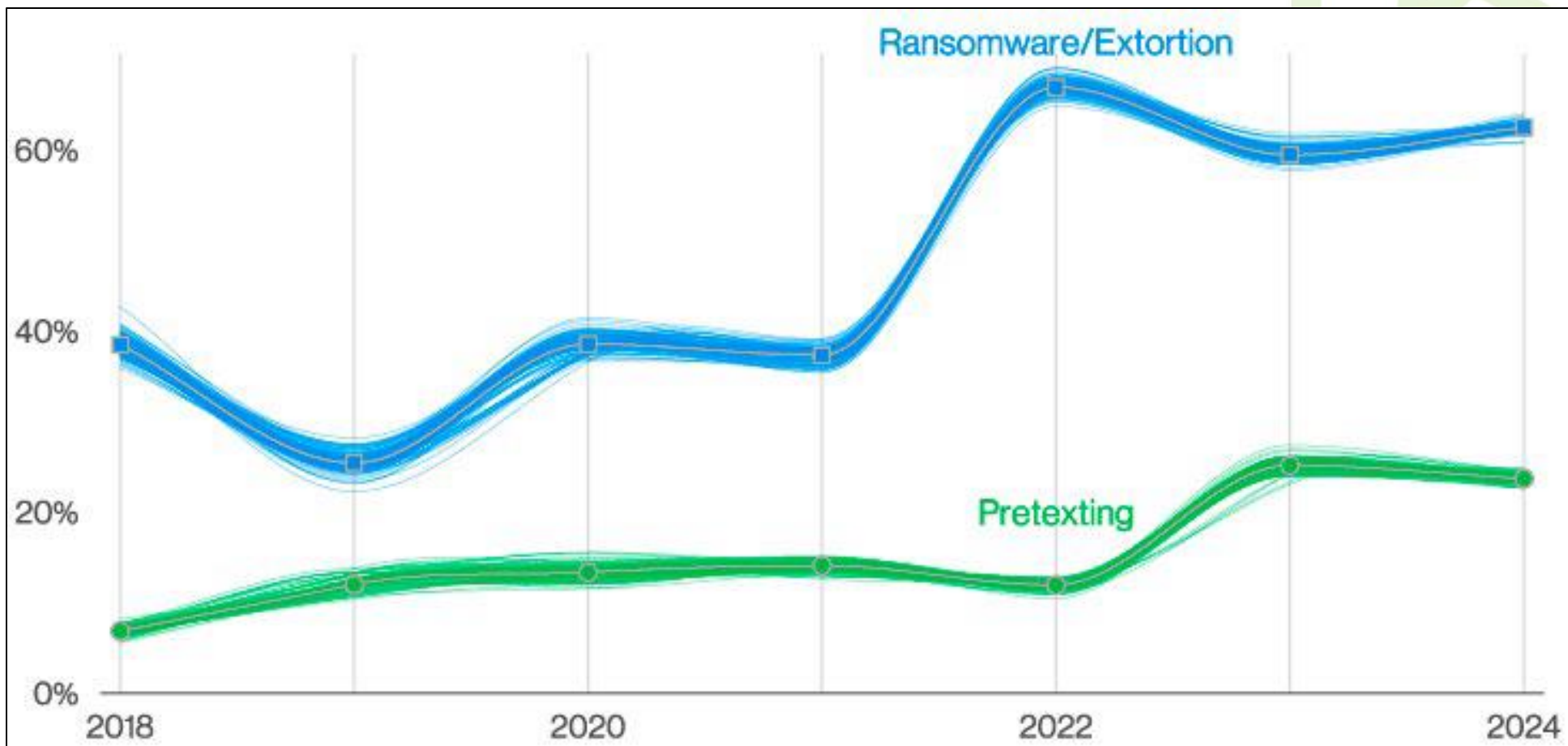
By the Numbers | Breaches



- 68% of breaches included a human element.
- 32% of breaches involved Ransomware or Extortion
- 28% of breaches involved Errors, e.g., misconfiguration
- 15% of breaches involved 3rd parties, e.g., supply chain, a newly added category to this report.



Ransomware Trends

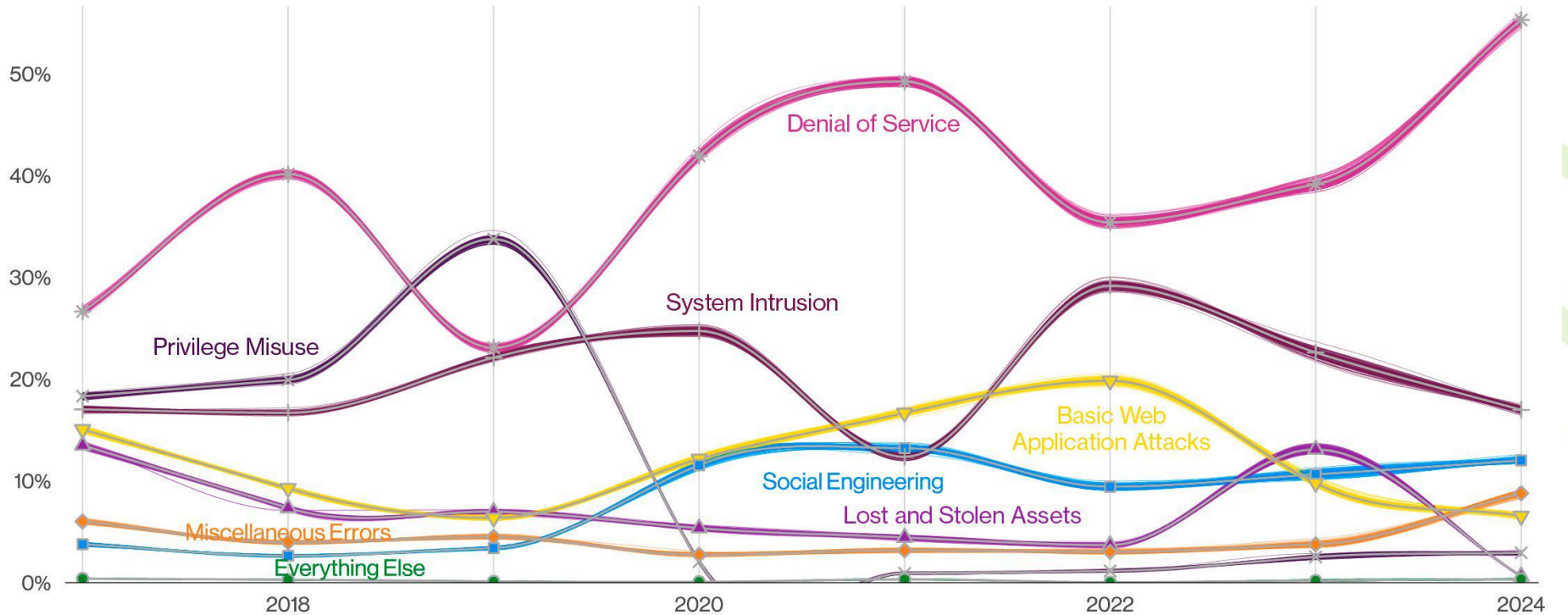


2024 Data Breach Investigation Report (DBIR) | Verizon



SECURECYBER
Proven. Proactive. Personalized.

Incident Trends

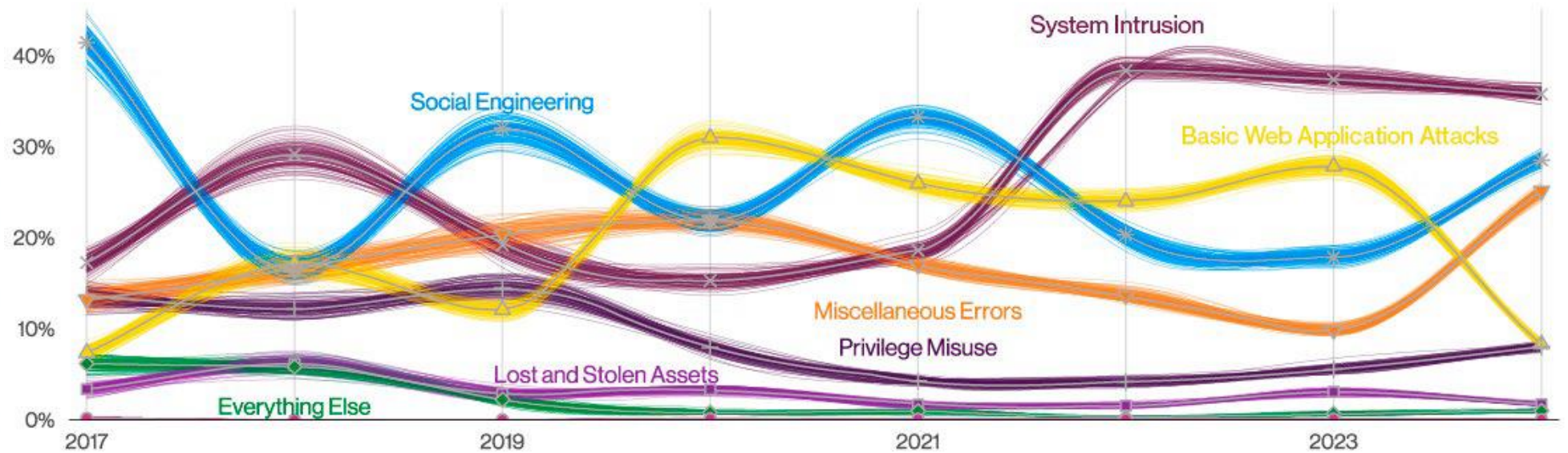


2024 Data Breach Investigation Report (DBIR) | Verizon



SECURECYBER
Proven. Proactive. Personalized.

Breach Trends

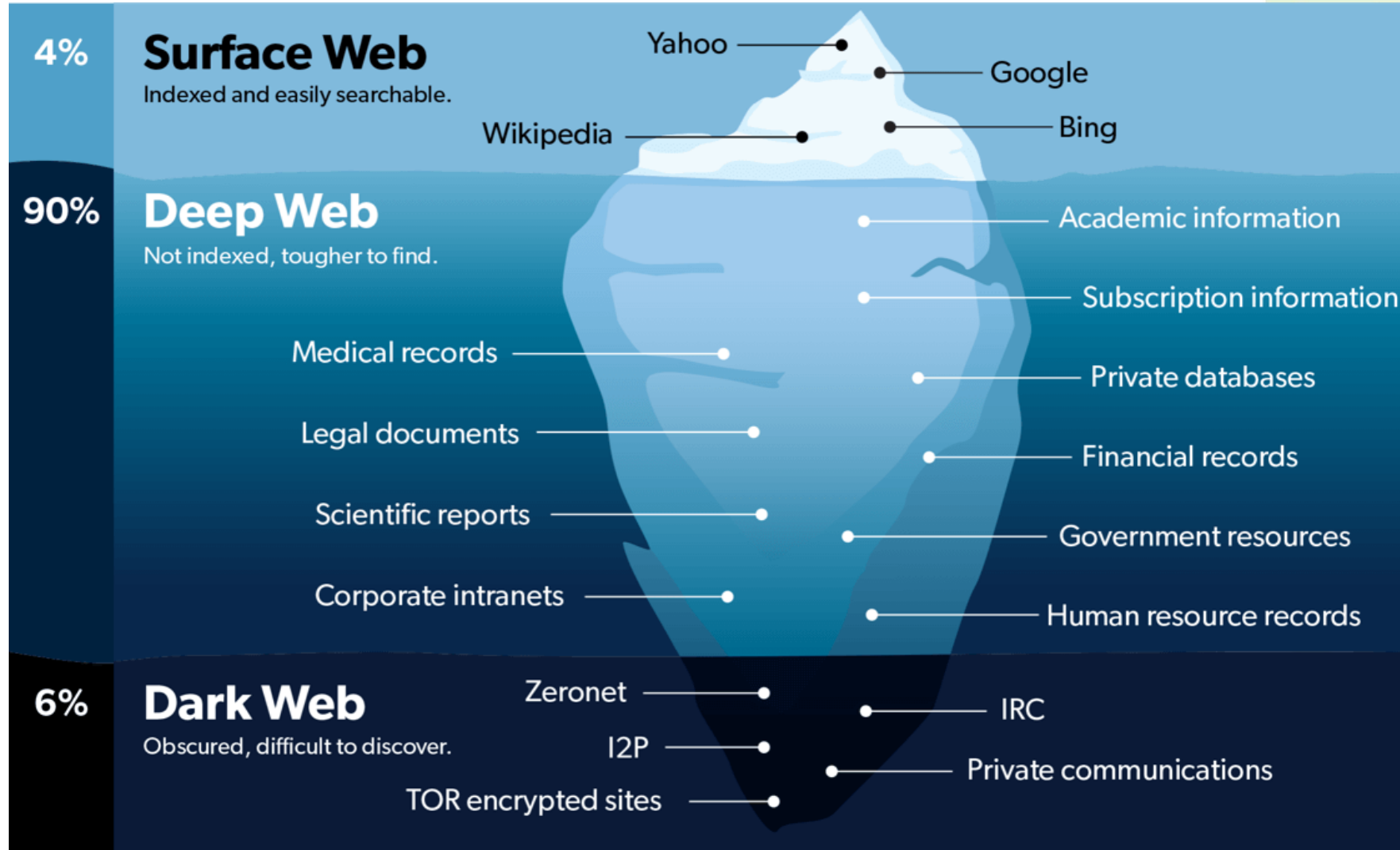




The Web Surface, Deep & Dark Web



Web in Layers



Dark Net/Dark Web

- Not searchable via search engines
- Requires anonymizing browser called Tor to access
- Digital underworld of illegal activity, malware and viruses, scams/fraud, hacking/surveillance, psychological harm, and more.
- A complex and dangerous place that should not be accessed.



SECURECYBER
Proven. Proactive. Personalized.

Top Dangers of the Dark Web

- Malware
- Legal Consequences
- Financial Scams
- Blackmail
- Exposed Personal Information/Credentials





Threat Actors & Threat Vectors

Threat Actors | Motivations

Cybercriminals

- Financial Gain

Thrill Seekers

- Satisfaction

Nation-States

- Geopolitical

Hacktivists

- Ideological

Terrorist Groups

- Ideological Violence

Insider Threats

- Discontent/Grudge

Common Ground:

- All are motivated in one way or another.
- All are opportunists and will take advantage of one or more exposure points to achieve their goal.



What is a Threat Vector?

(How it's done)

- Methods used by Threat Actors to gain illegal, unauthorized access to computer systems and networks, etc., including:

- Ransomware
- Phishing
- Missing/Poor Encryption
- Missing/Poor Patching
- DDoS
- Compromised Credentials
- Brute Force
- Software Vulnerabilities

- Malicious Documents
- Social Engineering
- Supply Chain Attacks
- Remote Applications
- Session Hijacking
- Insider Threats
- Email
- Malware





Threat Vectors Explained

Ransomware

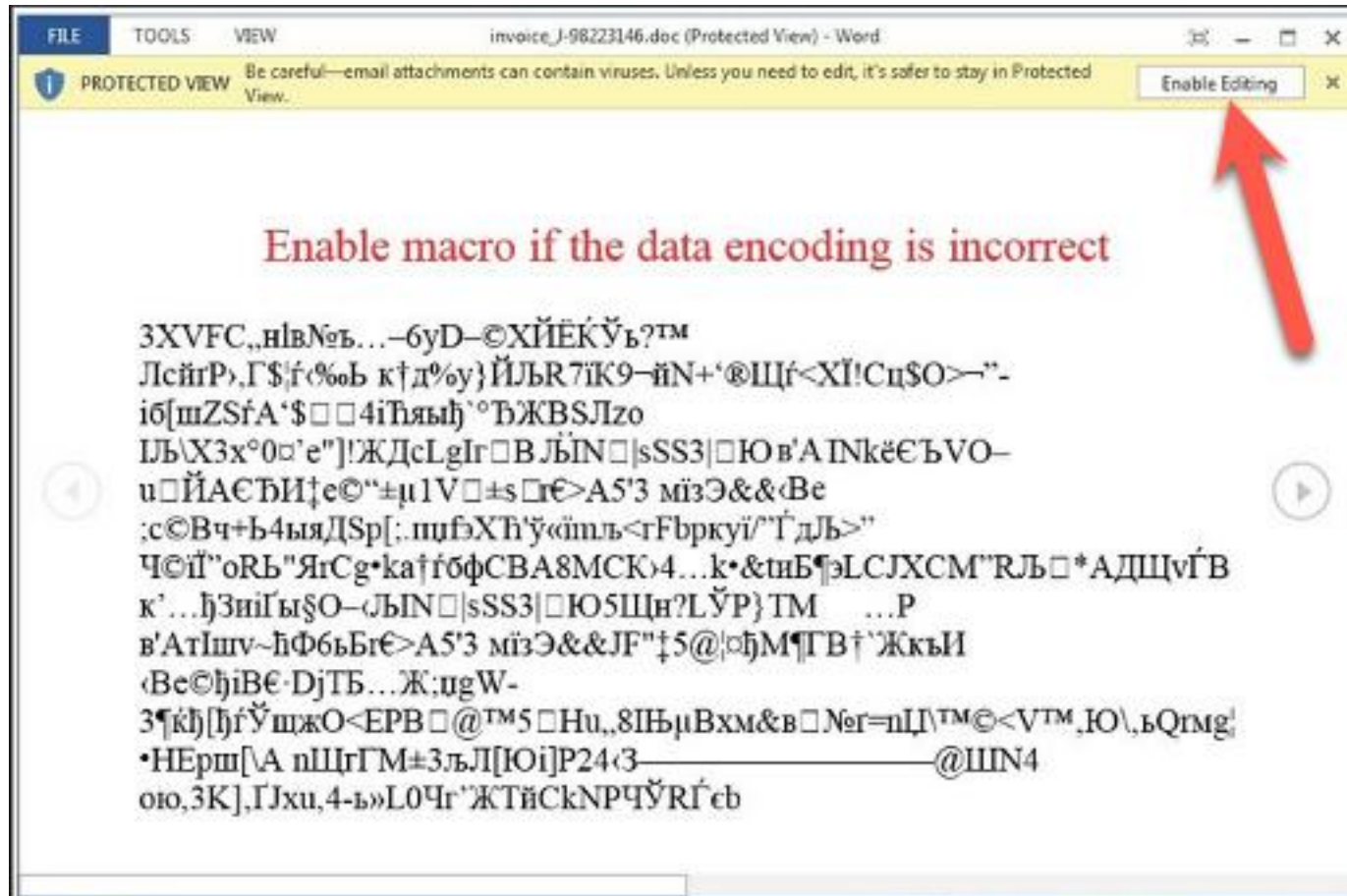


- Type of malware that prevents or limits users from accessing their system.
- It forces its victims to pay the ransom through certain online methods in order to grant access to their system, or to get their data back.
- Some ransomware encrypts files (called Cryptolocker).



Malicious Document

“Locky” Ransomware



Threat Actors want you to click to and enable macros.

DON'T ENABLE!!!



Emails & Phishing

- Fake email
- Appears to be a ‘trustworthy entity’ or ‘trustworthy individual’ asking you via email to perform an action
 - provide sensitive information such as SSN, credit card numbers, login IDs or passwords
 - requesting authorization of transfer funds
 - requesting gift card codes/pins, etc.



How to Detect a Bad Email

Cyber criminals might send an email that looks legitimate, known as a phishing email, but you can take steps to avoid the traps

The screenshot shows an email interface with several red boxes highlighting suspicious elements and blue callout boxes with labels:

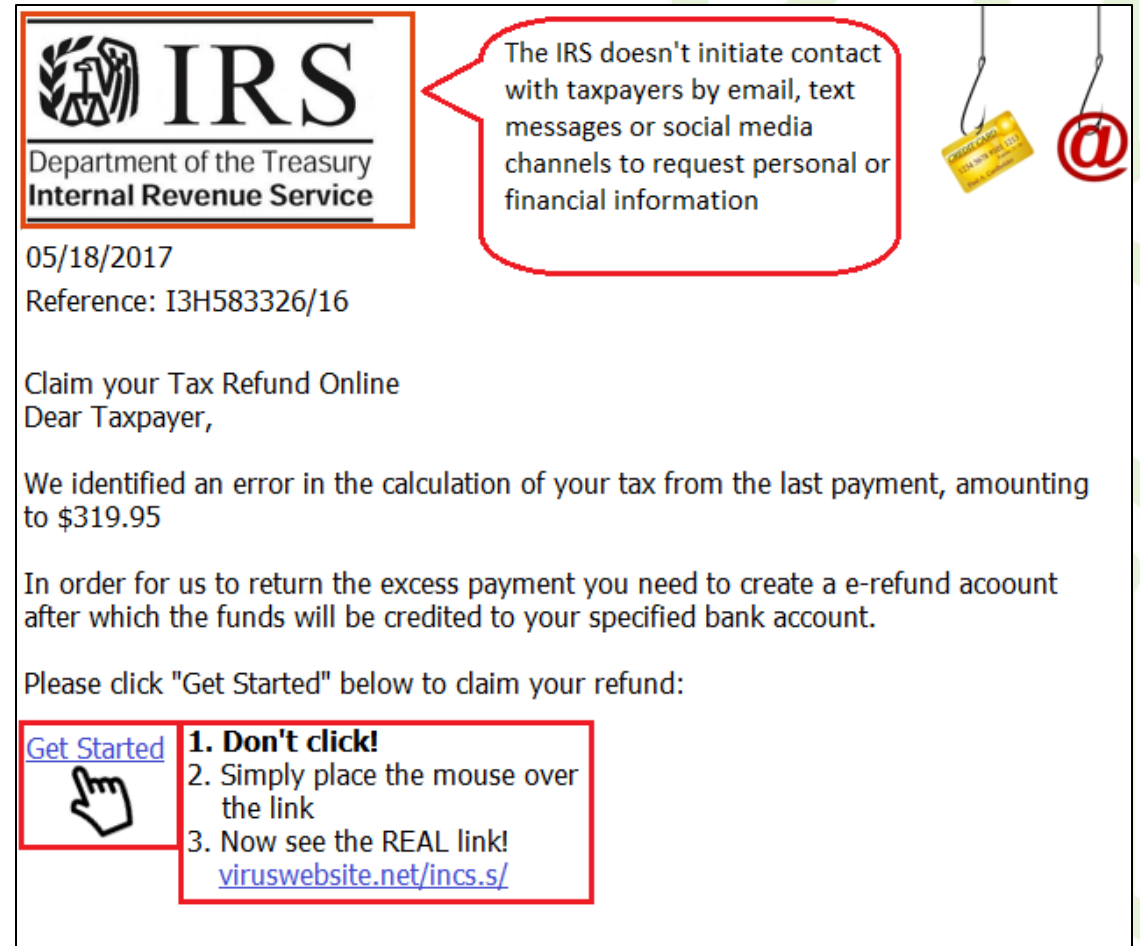
- FAKE EMAIL ADDRESS:** A red box highlights the sender's email address, `office-365@security.onmicrosoft.com`.
- CONTAINS VIRUS:** A red box highlights an attachment labeled "invoice.pdf" (2 MB).
- TOO GENERIC:** A blue callout box points to the salutation "Dear Customer".
- URGENCY:** A blue callout box points to the phrase "Invoice due now".
- POOR GRAMMAR:** A blue callout box points to the phrase "whats included".
- BAD LINKS:** A blue callout box points to a link that reads "http://66.160.154.156 /invoice Click or tap to follow link.".

The email content includes the Office 365 and Microsoft logos, the subject "Your Office 365 Business Essentials", and a footer with Microsoft Corporation contact information and an "Unsubscribe" link.



Emails & Phishing, cont.

- Threat Actors are opportunistic – e.g. tax time, holidays, Covid, disasters, election years, etc.
- Red Flags:
 - email from an agency that does not use email for notifications
 - bad link



The screenshot shows a phishing email from the IRS. A red box highlights the IRS logo and name. A callout box explains that the IRS does not initiate contact via email, text, or social media. A yellow tag with a red '@' symbol is also present. The email body contains a date, reference number, and a link to 'Claim your Tax Refund Online'. A red box highlights the 'Get Started' link and a list of instructions, including a suspicious URL: viruswebsite.net/incs.s/.

IRS
Department of the Treasury
Internal Revenue Service

05/18/2017
Reference: I3H583326/16

Claim your Tax Refund Online
Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to \$319.95

In order for us to return the excess payment you need to create a e-refund account after which the funds will be credited to your specified bank account.

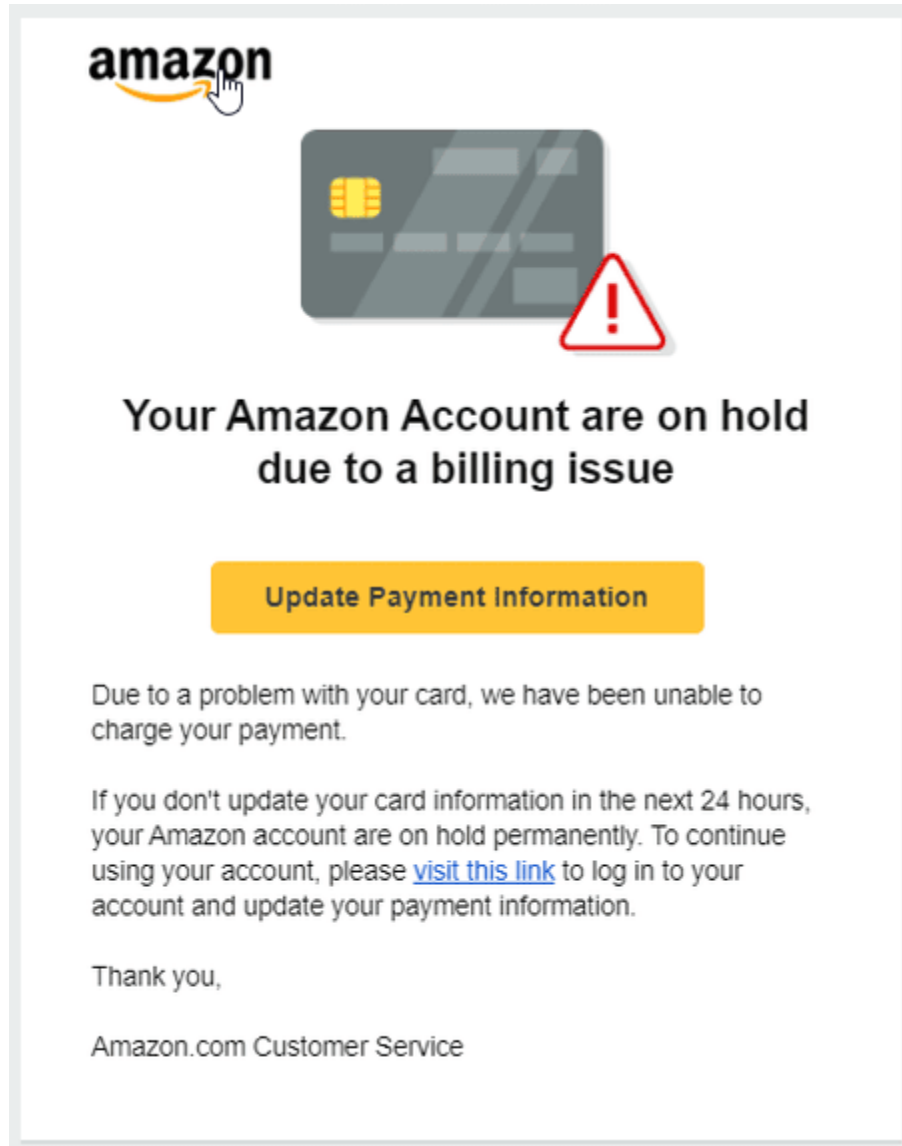
Please click "Get Started" below to claim your refund:

[Get Started](#)

1. Don't click!
2. Simply place the mouse over the link
3. Now see the REAL link!
viruswebsite.net/incs.s/



Emails & Phishing, cont.



- Phishing using common businesses we all know, e.g., Amazon, Netflix, PayPal, and many more
- Red Flags:
 - Urgency
 - Button to update payment information



Malicious Domains

- Confusing/similar domain names (squatting)
 - google.com v. goggle.com
- Cybersquatted domains resembling Apple.com, for example, led to malicious content more 70% of the time
- Cybercriminals conducting a domain war*
 - registering thousands of domains daily
 - phishing, scams, malware, and potentially unwanted program (PUP) distribution, adversarial search engine optimization (SEO), and distribution of illicit content*



Malicious Domains - Squatting

Often used for phishing campaigns, identity theft and malware install attempts.

Description	Examples
Typosquatting	whatsapp.com v. whatsalpp.com
Combosquatting	Popular trademarks abuse by adding words e.g., netflix.com v. netflix-payments.com
Homographicsquatting	Taking advantage of internationalized domains where Unicode characters are allowed (such as microsoft.com)
Soundsquatting	forever21.com v. 4ever21.com
Bitsquatting	microsoft.com v. micposoft.com
Levelsquatting	safety.microsoft.com.mdmfmztwjj.l6kan7uf04p102xmpq[.] bid v. safety.microsoft.com



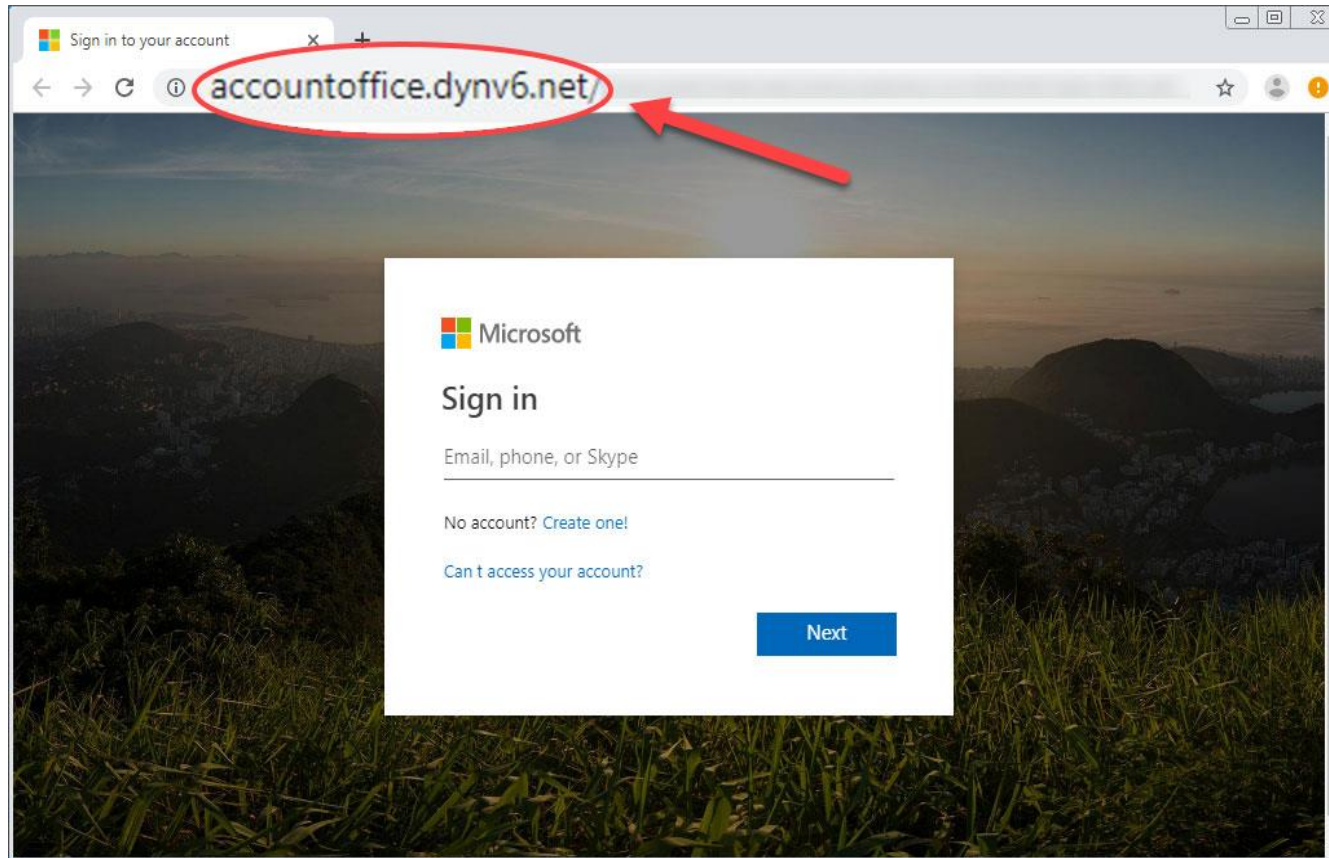
Ad Spoliation

The screenshot shows a Google search for 'freecad'. The search bar contains 'freecad' and is highlighted with a yellow box. Below the search bar, there are tabs for 'Images', 'Videos', 'Download', 'Tutorial', 'Perspectives', 'Review', and 'System requ...'. The search results show 'About 11,100,000 results (0.37 seconds)'. A red circle highlights a 'Sponsored' result for 'freecad-us.org' with the title 'FreeCAD Official Website - 2023 FreeCAD (CAD) - FreeCAD'. A red arrow points from the word 'Fake' to this sponsored result. Below it is a 'Real' result for 'FreeCAD' with the title 'FreeCAD: Your own 3D parametric modeler'. A red arrow points from the word 'Real' to this result. The 'Real' result includes a 'Download now' button and a 'Tutorials' link.

- Can be difficult to identify as fake
- Confusingly similar domain names
- Google reports in 2022 it:
 - Removed 5.2B ads
 - Restricted 4.3B ads
 - Suspended 6.7M advertiser accounts
 - Blocked/removed 1.36B advertisements for violating its abuse policies
- Recommendations:
 - Take your time to evaluate
 - Follow your instincts
 - Don't follow ads without scrutiny
 - Visit verified websites



Pharming – Fake Web Pages



- The link provided in the e-mail leads to a fake webpage which collects important information and submits it to the owner.
- The fake web page looks like the real thing
 - Extracts account information



Malicious QR Codes

- Quishing or QR Code phishing is when hackers trick users to exfiltrate their sensitive data . Upon scanning a malicious QR Code, uninitiated users submit their private information or download malware onto their mobile devices.



What is a Social Engineering Attack

- Manipulating individuals into performing actions that compromise security, e.g.
 - Divulging confidential information
 - Downloading software
 - Visiting websites that should not be visited
 - Sending money to criminals
 - Making other inadvertent mistakes that compromise personal or organizational security

Social Engineering Types

- Phishing
- Vishing
- Spear Phishing
- Pretexting
- Whaling
- QRishing
- Baiting
- Tailgating
- Watering Hole
- Smishing
- Scareware
- Pharming
- Quid Pro Quo
- Physical Breach
- DNS Spoofing
- Email Hacking



Steps to Avoid Social Engineering

- Slow down and be skeptical/follow your instincts
- Verify identity
- Use strong authentication
- Don't share confidential information
- Question urgency or pressure
- Beware of unexpected links/documents
- Secure social media
- Verify requests for money/data



Avoid Social Engineering & Malicious Software

- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their identity.
- Only visit and/or download software from web pages you trust.



Social Engineering/Media

Reported fraud losses by contact method

January 2021 - June 2023

More money was reported lost to fraud originating on social media than by any other method of contact.



Not shown are contact methods classified as other, including TV or radio, print, fax, in person, and other methods consumers write in or that cannot be otherwise categorized.



SECURECYBER
Proven. Proactive. Personalized.

Social Engineering/Media, cont.

- Limit who can see your posts and information
 - All platforms collect information about you based on activities
- Phishing scams
 - avoid links in DMs, email, posts, or text messages
- Scrutinize friend invitations
 - unknown persons
 - persons you are already friends with (likely account has been hacked)



Remote Access/Management Tools



- While remote access tools are often used by organizations for legitimate business practices, they are also popular for cybercriminals.
- Malicious actors will use remote access tools to establish network connections, escalate permissions, transfer malicious content, and more.
- Can bypass AV/EDR defenses, as they generally blend into legitimate business use.
 - AnyDesk 2/2024 Breach



Remote Access/Mgmt Tools, cont.



- Never give anyone you do not know access to your devices
- Never trust a call you were not expecting
- Don't trust anyone you do not know or have not verified asking for access to any of your devices
- Don't trust anyone you do not know or have not verified directing you to download specific software
- Never share information, e.g., credentials, banking information, OTP codes, or the like, with anyone



Malware Detection



- Red Flags

- Changes to your browser homepage/start page
- Ending up on a strange site when conducting a search
- System-based firewall is turned off automatically
- Excessive pop-up windows
- New icons, programs, and favorites which you did not add
- Frequent firewall alerts about unknown programs trying to access the Internet
- Bad/slow system performance



Artificial Intelligence (AI)



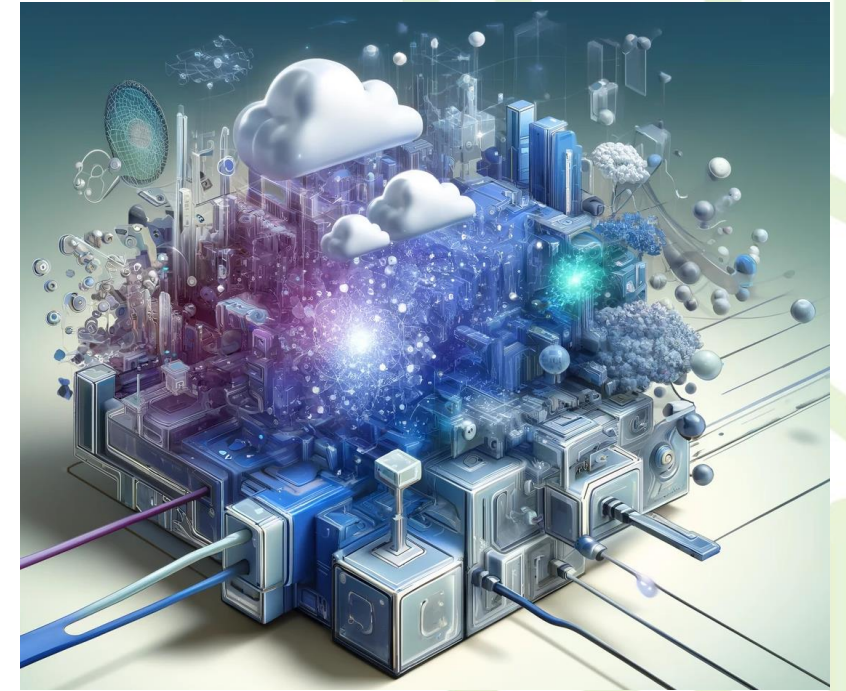
Positive impact to healthcare, retail, marketing, manufacturing, transportation, logistics, education, cybersecurity, construction, finance, entertainment, and many more

- AI is all the buzz...
- Benefits include:
 - Reducing human error
 - Improved automation
 - Less time in handling big data
 - Quick decision-making
 - Improved processes/workflows
 - 24/7/365 availability
 - and more



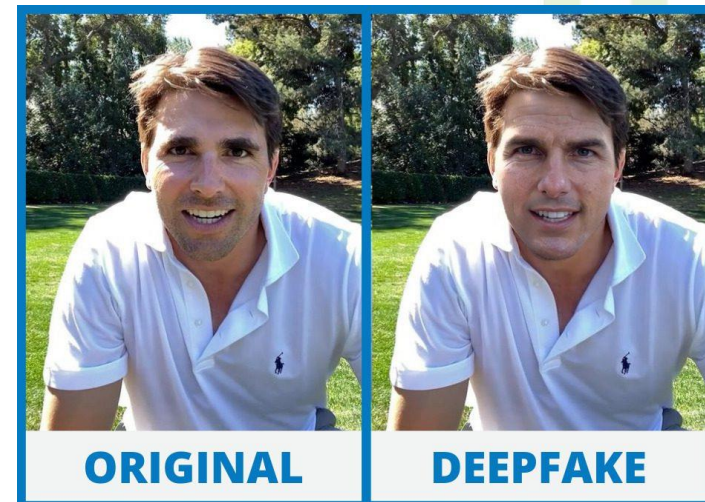
Artificial Intelligence (AI)

- With new or evolving technology, you get the bad with the good
- Malicious actors are using AI to take criminal activity to the next level, for example:
 - Generative AI
 - Highly realistic and convincing phishing emails, AI reading HTML of legitimate web pages and generating fake content
 - Sophisticated deep fake videos, manipulating of visual and audio content to deceive viewers



The Deep Fake

- The threat of deepfake videos comes not from the technology used to create them but from people's natural inclination to believe what they see online. As a result, deep fakes do not need to be particularly advanced to be effective in spreading mis/disinformation or to deceive its targets.
- Carefully examine suspicious videos. If you know what to look for, you can typically spot inconsistencies in deep fake videos.
- The warning indicators are:
 - Abrupt movements
 - Brightness shifts from frame to frame
 - Skin color shifts
 - Weird blinking or no blinking at all
 - Terrible lip-sync



Deep Fake

- Video
<https://www.youtube.com/watch?v=F4G6GNFz0O8>
- Deep Fakes are:
 - More sophisticated
 - Improving in quality
 - Harder to detect as fake
 - Can you trust what you see?



Online Shopping/Shopping Apps

- Carefully consider the sites you shop
 - Online shopping fraud is on the rise
 - Fake websites, fancy ads, ‘too good to be true deals’, and more
 - Questionable sites and/or shopping apps that may be doing much more than taking your payment for a product



Online Shopping/Shopping Apps, cont.

- Personal Data Access
 - Review permissions requests by apps
 - Only allow necessary data
- Security Concerns
 - Malicious apps infecting smartphones with harmful programs/malware, unexpected emails/texts you did not write
 - Consider a security app that scans and removes malicious software



Online Shopping/Shopping Apps, cont.

- Additional Software
 - Caution when clicking download buttons/links - avoid suspicious sites
 - Some sites install bundled and potentially unwanted programs alongside with the intended file download
- Research the Application
 - Look for recent data breaches or privacy issues associated with an app or parent company
 - Look at an app's track record
 - Make informed decisions on what you download/install
- Keep Applications Updated
 - Regularly update your smartphone's operating system and apps.
 - Updates frequently include security patches to address vulnerabilities - helps to safeguard your data and device





Threats in the News

Exploiting Home Devices



January 2024 Report – DOJ conducts court-authorized disruption of Russian hacking group ‘Fancy Bear’ botnet

- Moobot malware infecting more than 1K Ubiquiti routers in homes and small businesses
 - Malware variant infecting D-Link routers
- Targets routers with factory settings and weak passwords
- Purpose: conduct cybercrimes, including spear-phishing, credential harvesting, and more
- The DoJ urges users to complete a factory reset on affected routers, perform updates, and change of default administrator passwords



Exploiting Home Devices, cont.



January 2024 Report -
China's Volt Typhoon spies
infect hundreds of outdated
Cisco and Netgear devices
with malware

Purpose:

- Install VPN module to vulnerable devices
- Setup encrypted communication to remotely control botnet
- Potentially carry out attacks against US critical infrastructure
- Evade detection



\$25.6M Payout – CFO Deep Fake

February 2024



- Finance worker | multinational firm
- Threat actor, using deep fake technology, poses as company's CFO
- Worker duped into attending video call, including several other members of staff familiar to the employee – all deep fake creations
- Voices of executives.



\$25.6M Payout, cont.

- While initially suspicious upon receiving a message purportedly from the company's UK CFO, put aside doubts after the video call
- Investigation revealed the likelihood that threat actors relied on publicly available company videos and audio to digitally recreate the likenesses
- As video conferencing has become routine, cloning of meetings via realistic deep fakes poses a growing threat



Lawsuit – Popular Shopping Website

Questionable Activities

- Temu

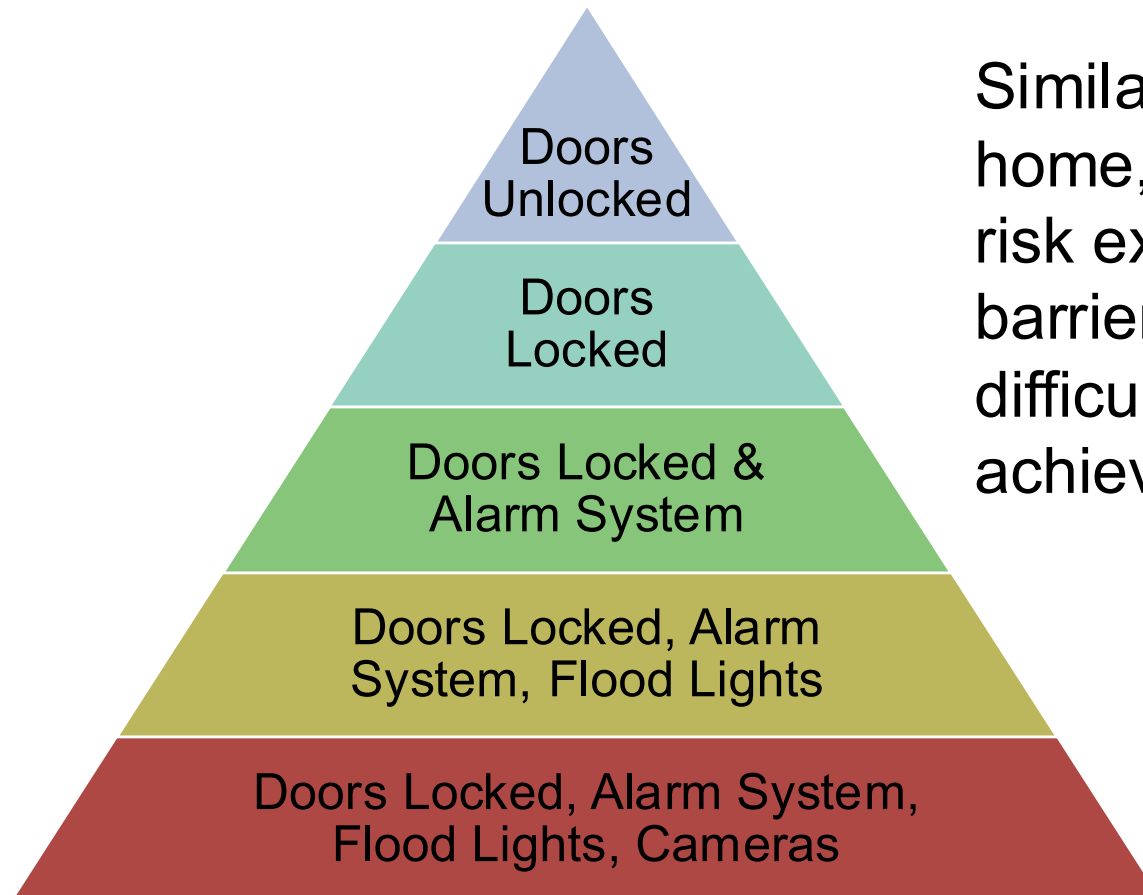
- Well-known Chinese e-commerce platform
- Class-action lawsuit accuses Temu of gathering personal customer data without proper notification and employing deceptive methods to access it. Additionally, the lawsuit asserts that Temu's mobile application harbors malicious software, including malware and spyware, posing significant threats to customer security, and potentially exposing them to identity theft and financial fraud.
- The lawsuit accuses Temu of violating multiple privacy and consumer acts





Cybersecurity Safeguards

Enhance & Maintain Good Cybersecurity Posture



Similar to protecting your home, you can reduce your risk exposure by adding barriers that make it more difficult for Threat Actors to achieve their goals.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

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	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years



> Hardware: 12 x RTX 4090 | Password hash: bcrypt

More difficult
the password
=
more difficult
to crack.

muffins
– instant

mIF@vMuFf1n\$
– 34,000 years



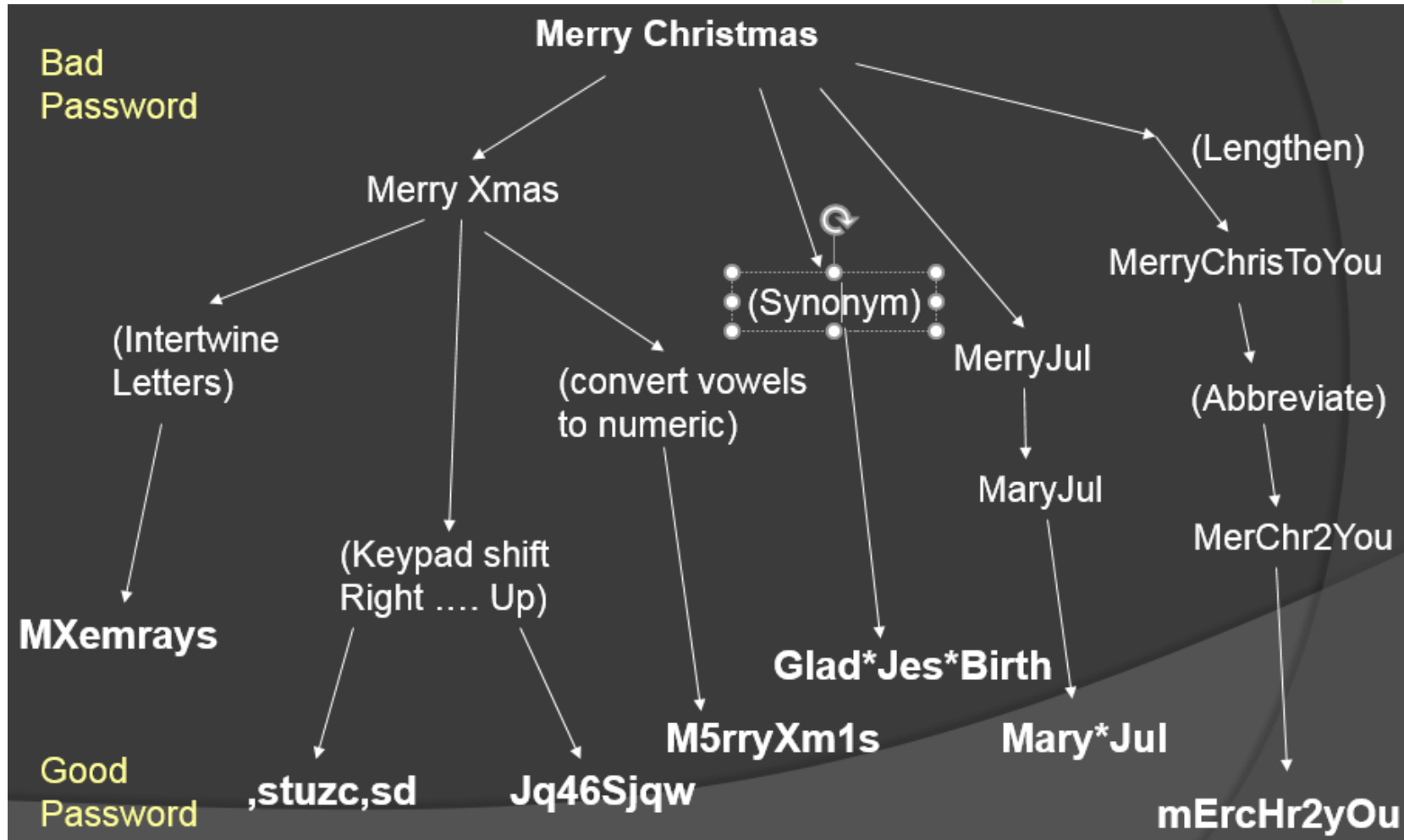
SECURECYBER
Proven. Proactive. Personalized.

Password Recommendations

- Never use 'password123' or 'password' or 'ilovepizza1!' as a login. A good password is:
 - Private: known to the owner only
 - Secret: does not appear in clear text in any form/media
 - Easily remembered: e.g., a passphrase only known to you, so there is no need to write it down
 - Changed regularly: a good change policy is every 3 months
 - Don't reuse passwords
- Be aware that someone may see you typing it. If you accidentally type your password instead of your login name, it may appear in system log files



Creating a Good Password



Password Generators

Password Generator: Easily Create Strong, Random Passwords

Use our free tool to generate unique, strong passwords. Just tap the dice!

<2z%u)@g[F!8%BxT{=^1Ev3<Qu2(M

Very Strong Password Copy

Character Length: 29

A-Z 0-9 !@#

See validation of
password strength.

Always check all available
options for complexity.



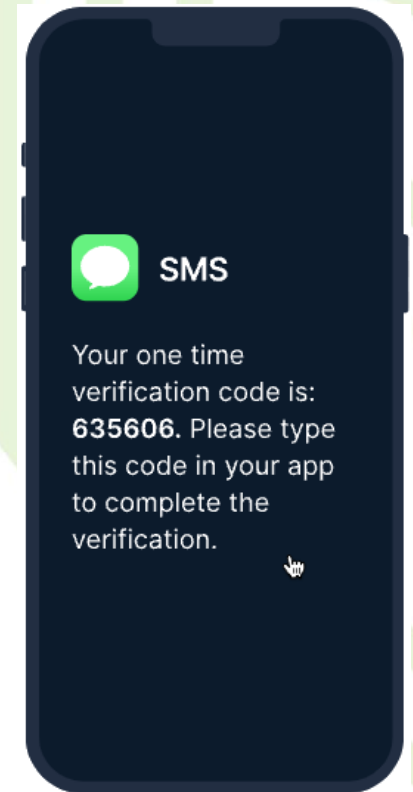
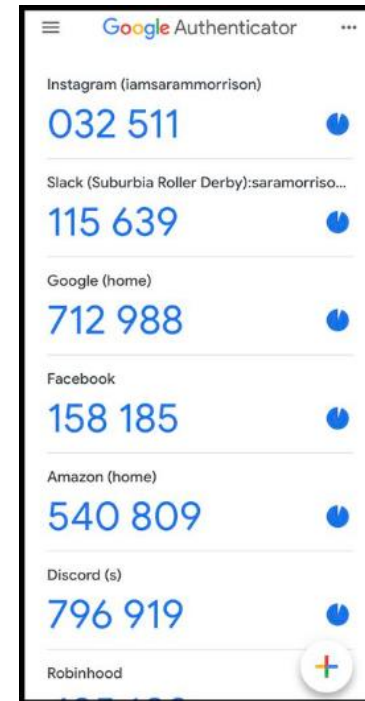
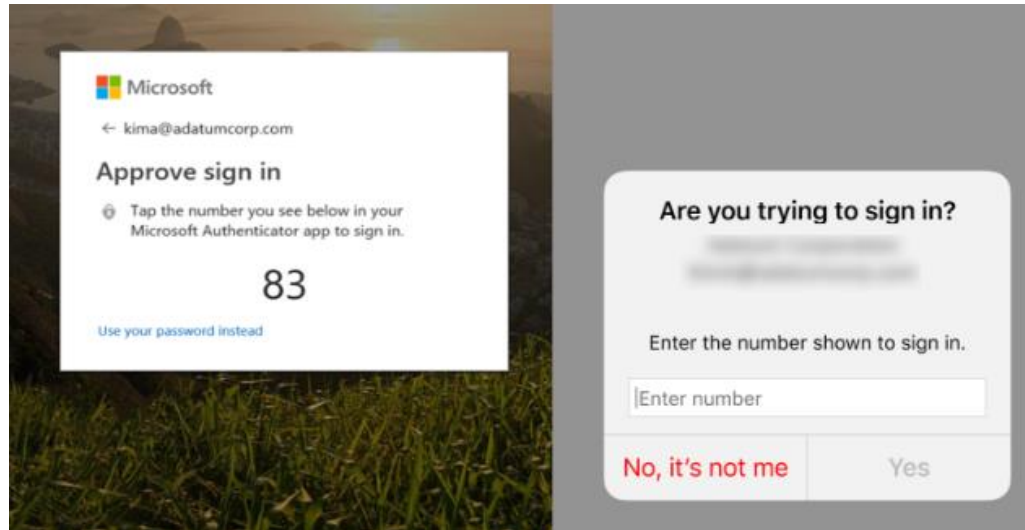
SECURECYBER[®]
Proven. Proactive. Personalized.

Password Managers



Multi-Factor Authentication (MFA)

- More than a username and password
- Includes a Text or Authenticator Apps
- Reduces the risk of password compromises



Common MFA Examples

- Time-based One-Time Password (TOTP)
 - Authenticator App
- SMS Text
- Email Token
- Hardware Key
- Biometric
 - Thumbprint/Face Recognition



Where do I setup MFA?

- EVERYWHERE!
- Business or personal
- Enable MFA for any login you have where the security feature is available.



No MFA is Unhackable

- As with many security solutions, if we build it, hackers will work to combat it. MFA is no exception.

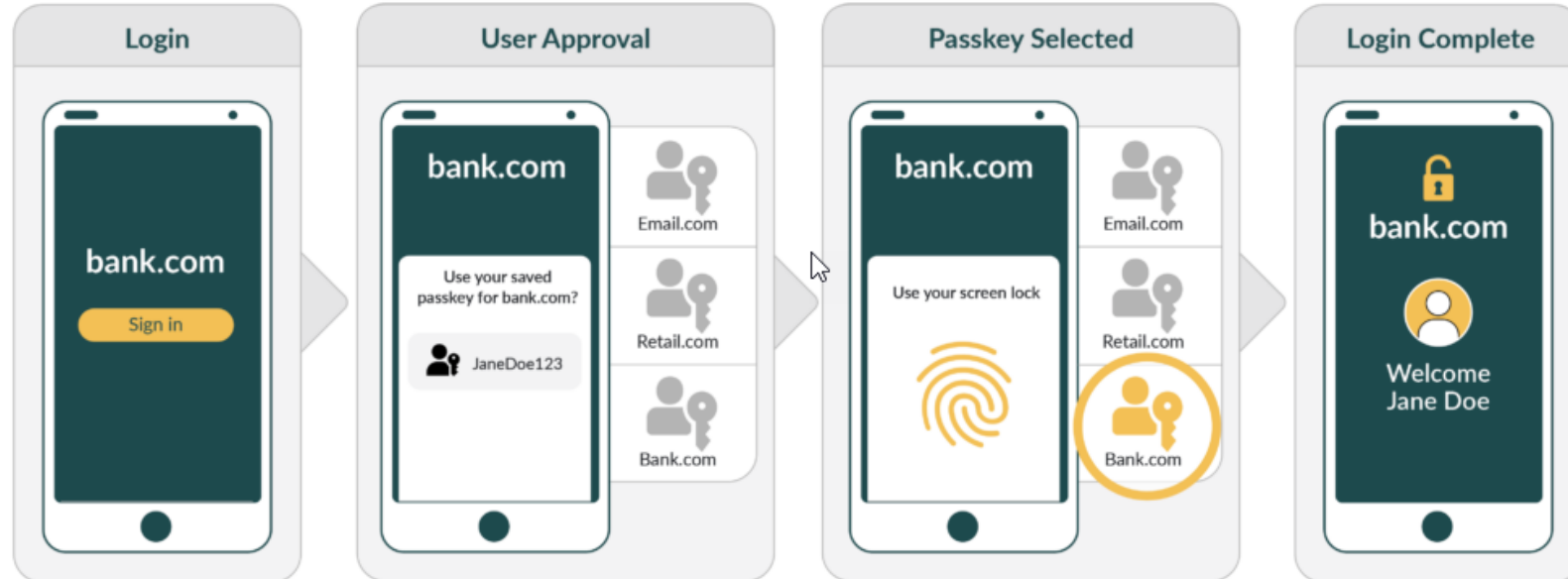


- Regardless, MFA should be enabled wherever possible. Threat Actors must work harder to compromise accounts when MFA is enabled, versus if you don't have it at all.
- New authentication mechanism gaining adoption to reduce risk of compromise – FIDO/FIDO2.



FIDO/FIDO2* Authentication

- FIDO takes this a step further by challenging any login attempt by requiring a private key which is only available on the authorized user's device.



*FIDO2 is supported by all leading browsers and operating systems.



Keep Your Home Network Safe



Key Steps to a Safe Network

- Consider what you need
- Secure Your Wi-Fi
 - Separate private/guest wifi use
 - Consult product guides for capabilities
 - Monitor your network
- Keep up with Firmware, Patches and Updates
 - Kids devices, Apple Devices, TV's, Keurig, Washer/Dryer
 - aka IOT (Internet of Things)
- Manage passwords
- Use Password Managers (Keeper)
- Enable MFA



Cybersecurity-on-the-Go

- No to Public Wifi
- Yes to VPNs



- Top 10 Virtual Private Network (VPN) Apps
 - NordVPN
 - NetMotion
 - pfSense
 - ExpressVPN
 - Perimeter 81
 - ProtonVPN
 - OpenVPN Access Server
 - NordLayer





Situational Awareness

Situational Awareness & Social Engineering

- Important Information:
 - WATCH what is going on around you.
 - WATCH what you are posting to social media
 - REPORT anything suspicious
 - CLEAR your desks of sensitive information



Situational Awareness & Social Engineering, cont.

- Video
<https://www.youtube.com/watch?v=qkgN4Bwhpf8>
- Demonstrates
 - How easy it can be for a threat actor to gain access to a work environment
 - Things may be not what they seem – pay attention to the clues



Summary

The background is a dark green grid with glowing green light trails that curve and flow across the frame. On the left side, there is a faint, circular logo or emblem, possibly a university crest, rendered in a lighter shade of green.

Security-Minded Approach

- Zero-trust is a cybersecurity concept of never trust and always verify
- This concept can be applied in life as well
- Takes steps to protect both you and you're the organization you work for
 - Slow down
 - Scrutinize
 - Ask for help when in doubt





SECURECYBER™
Proven. Proactive. Personalized.

Thank you

For more information, please contact
sales@secdef.com



Shawn Waldman, CEO



Chad Robinson, VP Advisory



Kyle Zech, Sales Manager



Chris Randall, Account Manager