

Cybersecurity Awareness

Tips To Protect You And Your Data

ADAPTATION FROM:



TreeTop Security
Stand Above.

PRESENTED BY

KRIPESH LAMICHHANE

Senior IT Officer, NEFSCUN





Legal Disclaimer

While we'd love to boast that our cybersecurity awareness training is foolproof, the reality is no training can safeguard you from all cyber threats and that includes cyber criminal's relentless attempts to send you malware laced cat memes. It is, however, the best single hour you can use to learn ways to better protect yourself from the evil lurking on the digital interwebs. Your best defense against cyber-foolery is your own cyber-wisdom. Remain vigilant, keep your passwords as complex as the plot twist in a thriller movie, and learn to embrace your inner cybersecurity awareness ninja!



**LIVE
LAUGH
GET HACKED
STOP LAUGHING**

Overview



Why security awareness?

Backup, backup, backup

Patching ALL of your devices

Passwords

2-Factor Authentication (MFA)

Internet Safety & Email

Phone Scams

Privacy Concerns

What to do when things go wrong?



01

**Why is
cybersecurity
awareness
important?**



Awareness training is a must!

Technology alone ***cannot*** protect you from everything

Hackers go where security is weakest

People -> a link the chain & the last first line of defense

A must to reduce cybersecurity risk

Cybersecurity awareness is for...

- Employees
- Business Owners
- Parents
- Kids
- Seniors
- **Everyone!**



Reminder: Many tips that keep you safe at work will also keep you safe at home!

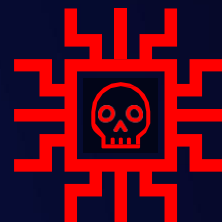


But an attacker isn't interested in me...



⊗ **Wrong!!! - You are exactly what an attacker wants!**

- Credit Card & Financial Data
- Medical Data
 - Prescription, insurance, or identity fraud
 - Far more valuable than financial data
- Computer Resources
 - Cryptomining
 - Advertising
 - Ransomware
 - “Jump Point”
- User or email credentials
 - Sending spam
 - “More” access
 - Recovery/Reset other accounts





02

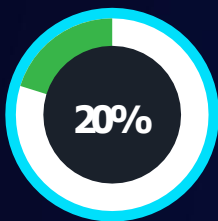
HELP!!!

**Ways to protect
yourself!**

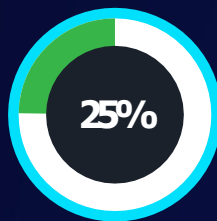


Backups

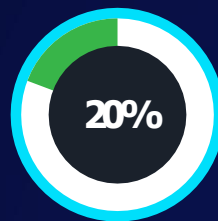
- Backups protect when all else fails
 - NO level of protection is perfect
 - Only “guaranteed” protection against ransomware
- Backup media should *not* be connected at all times
- Test your backups! Restore, restore, restore!



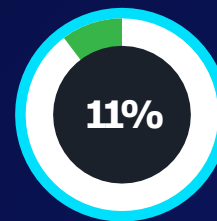
Users that have never backed up



Users that backup yearly



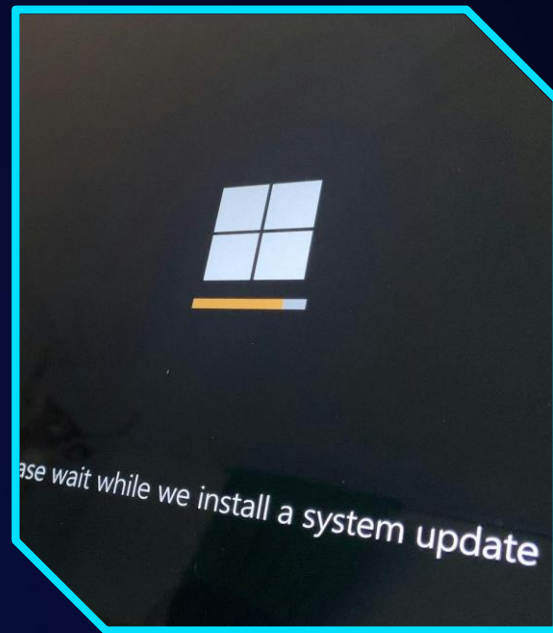
Users that backup monthly



Users that backup daily

Updates are essential to security.

- What was secure yesterday may not be secure today
- New software vulnerabilities are found every day
- Over **450,000** new malware (viruses & ransomware) released every day
- Nothing is “Set & Forget”



Keeping your system up-to-date

Operating Systems

- Microsoft Windows, Apple MacOS, Linux
- Windows 7 end of life was January 2020
- Windows 10 end of life? October 2025



Anti-Virus

- Update to the latest definitions to ensure protection against the latest threats
- Symantec/Norton, McAfee, Windows Defender, Avast, and many others!



Don't forget to update...

- Browser - your portal to the internet
 - Chrome, Firefox, Edge, Safari, Brave, etc.
 - ~~Internet Explorer~~ (Not recommended)
- Mobile devices - cell phones & tablets
- Internet of Things (IoT) - Alexa, Google Home, light bulbs, thermostats, doorbells, surveillance system, smart locks, pet feeder, vacuums, health monitors...
This list could keep going forever!





03

All About Passwords



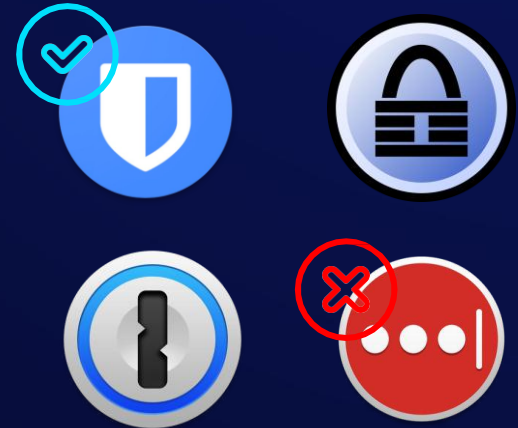
SOMEONE FIGURED OUT MY PASSWORD,



NOW I HAVE TO RENAME MY DOG

Managing Passwords

- Keep your passwords in a secure location
 - Do NOT use paper or sticky notes
 - Do NOT store passwords in clear-text on your computer - Word, Excel, etc.
- Utilize a password manager (aka vault)
 - **Bitwarden** ○ KeePass ○ LastPass
 - Chrome? ○ Apple Keychain?
- Benefits of a password manager
 - One strong password to access them all
 - Passwords are stored securely
 - Auto-fill username/password on websites
 - Sync between desktop, laptop, and mobile

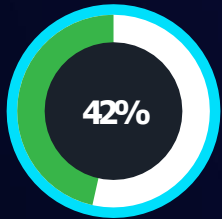


Password Tips

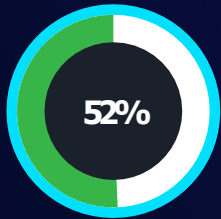


- Avoid using items that can be associated with you
 - Address
 - Phone numbers
 - Pet names
 - Child names
 - Birthdays
 - Sports teams
- Separate passwords for every account
- Auto-generated, near impossible to guess

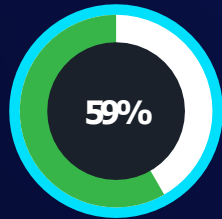
Much easier with a password manager!



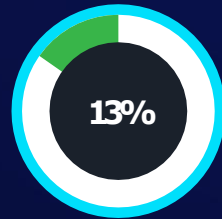
Rely on sticky notes for password mgmt



Re-use password for multiple accounts



Use name or birthdate in password



Reuse same password for all accounts



Passphrases, not passwords

- Useful when passwords must be typed in
 - Computer login
 - Wireless ← no phone numbers!
- Should not be easy to guess
 - At least 12 characters, but 15 or more is far better
 - Length better than “complexity” - upper, lower, number, & special characters (~!@#\$%^&* _-+=`|\(){}[]:;'"<>.,?/)
 - Bad password (8): P@ssw0rd
 - Great password (25): MysonwasbornNovember1995!



Why are most passwords exactly 8 characters?

Top 20 passwords by rank & year



Rank	2020	2021	2022	Rank	2020	2021	2022
1	123456	123456	password	11	1234567	qwerty123	1234567
2	123456789	123456789	123456	12	qwerty	000000	1234
3	picture1	12345	123456789	13	abc123	1q2w3e	1234567890
4	password	qwerty	guest	14	Million2	aa12345678	000000
5	12345678	password	qwerty	15	000000	abc123	555555
6	11111	12345678	12345678	16	1234	password1	666666
7	123123	11111	11111	17	iloveyou	1234	123321
8	12345	123123	12345	18	aaron431	qwertyuiop	654321
9	1234567890	1234567890	col123456	19	password1	123321	7777777
10	senha	1234567	123123	20	qqww1122	password123	123

If you use any of these, change them NOW!!!

Password Length ↔ Time to Crack



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	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Time for an attacker to brute force your passwords.

Are you in the  **yellow** or **green**?

MFA - Multi-Factor Authentication



What is MFA?

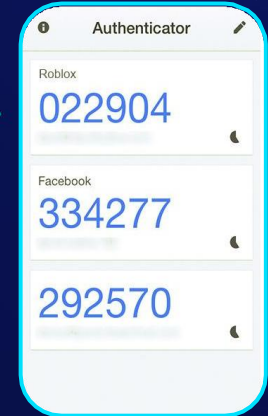
- “Beyond” a username and password
- Another form to prove it is you
- Typically out-of-band
- Can be biometric - fingerprint, facial, etc.

“Your one-time code is...”

- SMS (Not as secure)
- Email
- Phone Call (Not as secure)
- Phone Pop-Up
- Authenticator applications
 - Google Authenticator
 - Microsoft Authenticator
 - Built into a password manager?



Biometric - fingerprint or facial recognition



Authenticator apps

99.9% LESS likely to be compromised if you use MFA

MFA Under Attack

MFA Fatigue

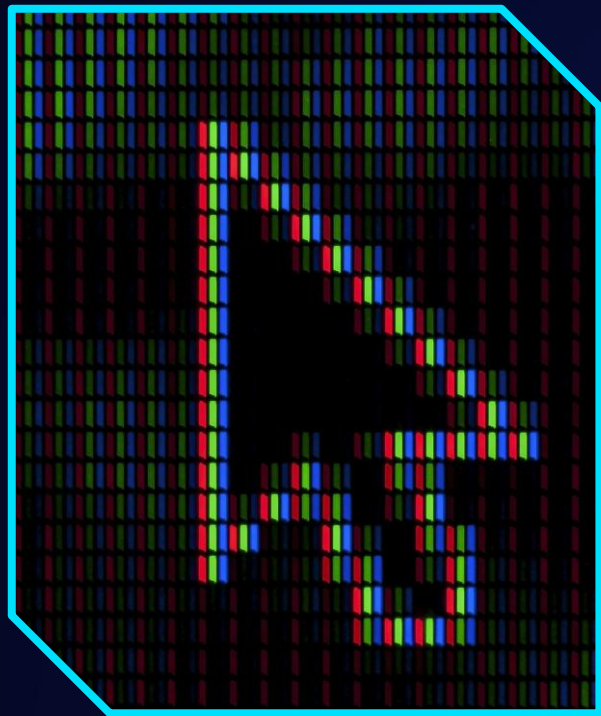
- Attacker targets the end user rather than jump through technical hoops
- Users overwhelmed by frequent authentication requests causing:
 - Frustration
 - Carelessness in approving prompts
 - Potential security risks
- Users may unknowingly approve malicious requests just to stop the prompts
- Your phone becomes unusable due to an MFA pop-up every 5 seconds. Would you click approve?



Authentication Best Practices



Method	Security Level	Recommendation
SMS / Text Codes	Moderate	Avoid if possible (Sim Swapping risk).
Authenticator Apps	High	Industry standard for employee accounts.
Hardware Keys (YubiKey)	Maximum	Required for critical admin access.
Biometrics	High	Excellent for mobile device local access.



04

Just a Little Click



Is the link safe in 4 steps

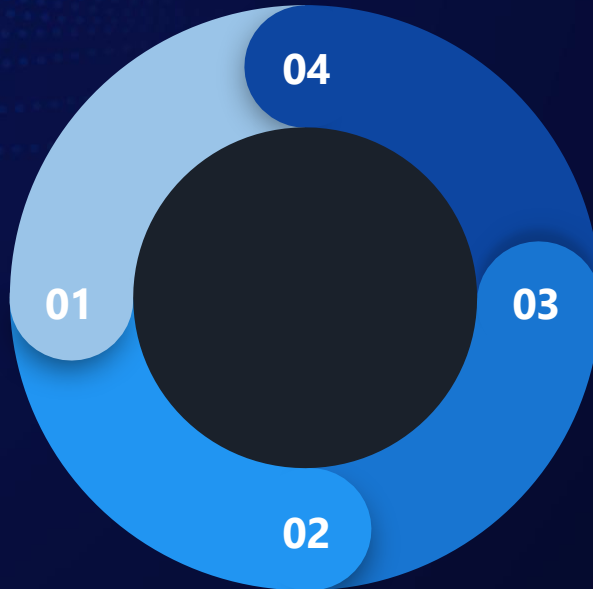
1. Verify

Were you expecting a link?

- Not just email!
 - Social Media
 - SMS/iMessage
 - Zoom, Teams, Slack, etc.
-

2. Hover

Hover over the link to ensure that it leads to where it says it does



4. Click

Does it pass all 3 tests?
Still use caution
“When in doubt, throw it out”

3. Sniff test

Is it a site you recognize?
Does it feel “familiar” to you?
Be skeptical



Easy to Recognize Scam

Everything is allowed! Just don't forget Viagra.



BEST CAN DRUGS <online_pillsshop5hfal@pharmacy.canada>

To: [Redacted]

[SHIP NOW \[RX-COMPANY\]](#)



Red flags? ->

Viagra <- !?!?!?

Strange Wording

Email Address

Domain Name

Expected email?

Interesting link

From a Known Email Account



**Hacked or Spoofed
email from someone
you know**

*Similar attacks via
Facebook & Social
Media*



Red flags? ->

Email address = OK

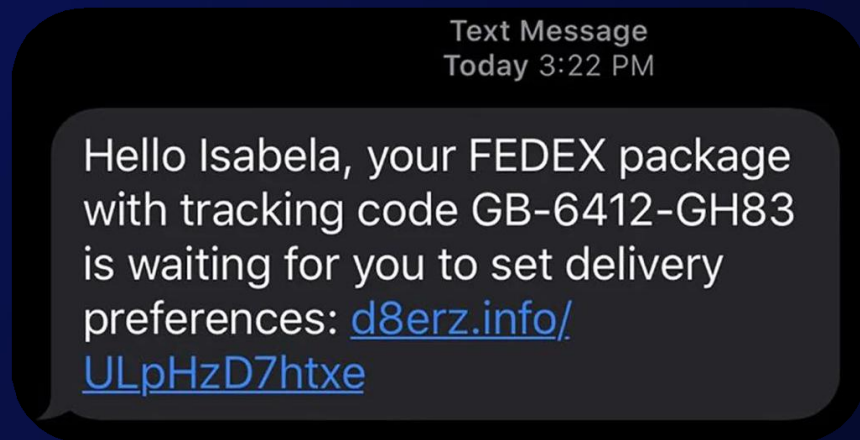
Name = OK

Odd "Signature"

Expected email?

Link -> .fr is France

Text Messaging Example



Red flags? ->

Name in SMS = OK

Number OK?

Expected Text?

Received a text regarding a package before?

Recognized domain?



Hover before you click

- Why hover?
 - Blue text can be deceiving
 - Underlying URL may be different
 - “Foreign” domains - .uk, .cn, or .ru
- Numbers instead of letters
 - Example: 192.168.1.1
 - Don't trust it!
- Hover on mobile/tablet?
 - Long press (hold)
- Any doubts? Don't click it!!!

Desktop
Hover
Example

www.treetopsecurity.com

Click to open in a new window or tab
<http://www.evil.com/>

Mobile
Long-Press
Example

<http://www.evil.com/>

Open

Open in New Page

Add to Reading List

Copy

Cancel



Shortened or Obfuscated Links?

Instead of 300 characters, the link is reduced to 15 characters.

- Bit.ly
- Cutt.ly
- TinyURL
- Many more!

Extremely Common and helpful, but...

Abused by criminals to hide malicious websites.

[Link Expander](https://www.expandurl.net/)

<https://www.expandurl.net/>



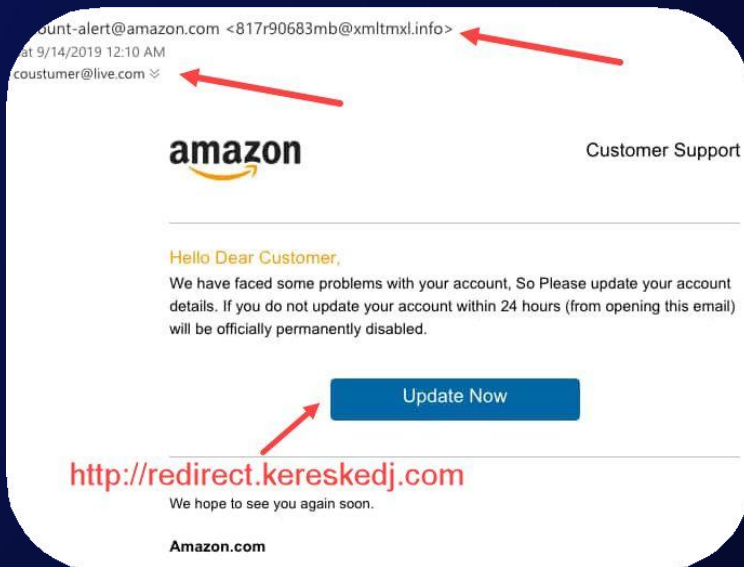
https://bit.ly/2Zppluc

Expand

Uncovered URL is:

<https://www.treetopsecurity.com/cybersecurity-awareness-training-feedback>

Hovering is your Friend



Red flags? ->

Email address OK?

Sense of Urgency

Expected Email?

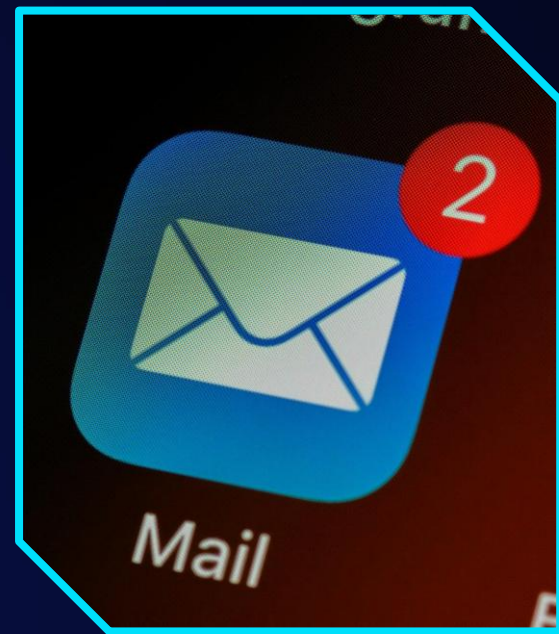
HOVER!!!

More Email Attacks

94% of malware is delivered by Email

1.2% of all emails sent are malicious

Over three billion phishing emails
every day!



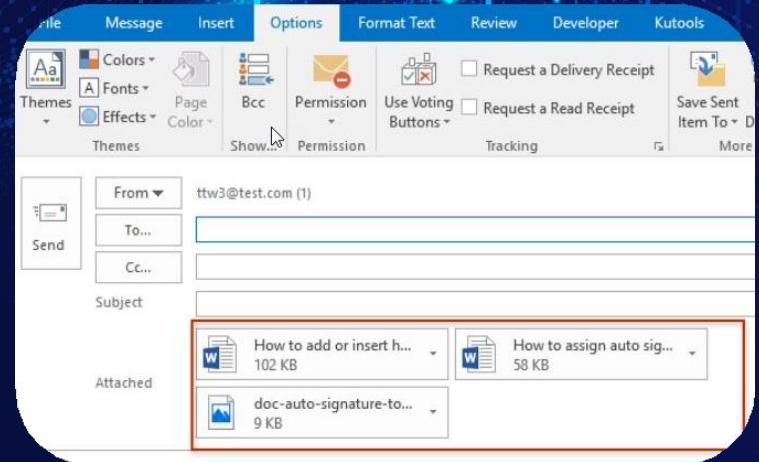
Email Attachments

- Stop & Think before you click!
- Recognized Sender?
- Expecting Attachments?
- Is it normal for that contact to send attachments?

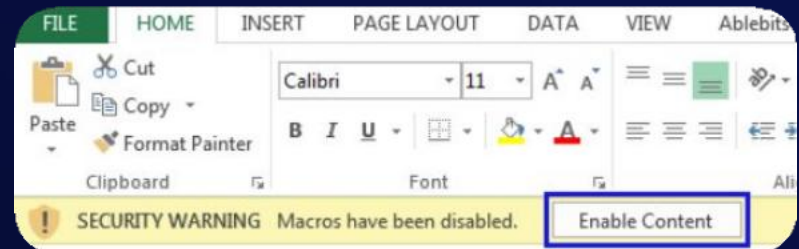
Macros

- Step 1: Don't do it!!!
- Step 2: Please See "Step 1"
- Found in downloaded files also

Attachments in email client (Microsoft Outlook)



🚫 Enable Macros <- NOOOOOO!!!! 🚫



Business Email Compromise (BEC)



- FBI: BEC cost businesses \$1.8B every year
- Moving funds -> more susceptible
 - Policy requiring phone call?
- “Trusted” senders
 - Research using publicly available data
 - Published organization chart
 - Spear phishing (CEO <-> CFO)
 - Spoofed domain
 - microsoft.com - micros0ft.com
 - Compromise account of 3rd parties
 - Employee, vendor, or customer
 - Thread hijacking <- lookout

Wire transfer

From: [Redacted]
Sent: Tuesday, March 28, 2017 1:21 PM
To: [Redacted]
Subject: INSTRUCTION FOR WIRE TRANSFER

Hi [Redacted]

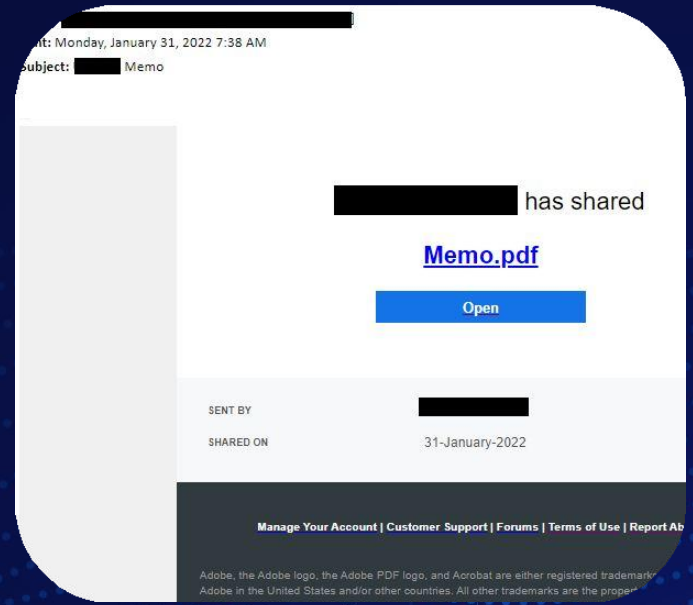
I need you to process a wire transfer to a new vendor.
please let me know when you can get it done

Thanks
[Redacted]

*Often requires very
little technical skill*

Customer BEC Example

- Small business < 100 employees
- CEO received email
 - From school district (their customer)
 - Bid proposal
 - Busy CEO blocked, certain it was legit
 - Asked us to “bypass” blocks/alerts
- Give us 5 minutes
 - Contacted school IT
 - “You’re the 2nd call”
 - All within 30 mins of 1st alert

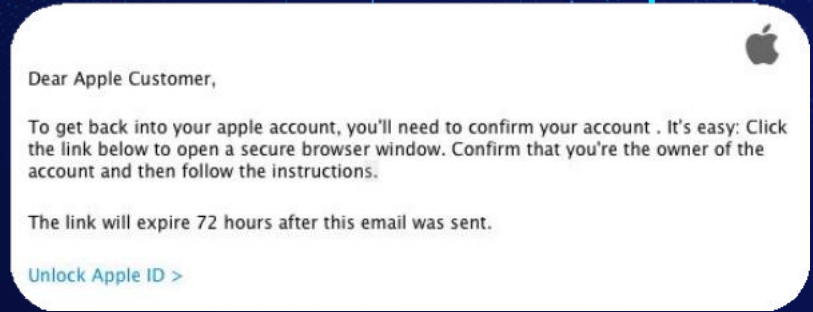


Other Email Scams

- Mostly “non-technical”
- What the attackers want
 - Money
 - Gift cards
 - Wire transfers
 - Access to email & accounts
- Possible signs
 - Sense of urgency
 - Never happened before
 - No limit on what they say/do



Account credential phishing attack



Technology alone
cannot solve this



Scammer Favorites

- Mimic recent, breaking news
 - Worldwide
 - Health scares (Ex: COVID)
 - Protests
 - Elections
 - Local and regional
- Seasonal/holidays
 - Order & delivery issues
 - Tax issues

Recent events

DT Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

[Safety Measures.pdf](#)

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr. [Redacted]
socialist wuhan-virus-advisory

Order Cancelled

amazon.com - Your Cancellation (193-2134-83111)

order-update@amazon.com
Today, 12:13 PM
You

Dear Customer,

Your order has been successfully canceled. For your reference, here's a summary of your order:

You just canceled order [193-2134-83111](#) placed on June 28, 2017.

Status: CANCELED

1 "Blumped": 2003, Deluxe Edition
By: Julian Moore

Sold by: Amazon.com LLC

Thank you for visiting Amazon.com!

Amazon.com
Earth's Biggest Selection.
<http://www.amazon.com>





05

Reach Out & Scam Someone

Phone Scams

Social Engineering, what is it?

- Banks & Credit Card Companies
- Medical & Insurance
- IRS or any past due account balance
- Objective: Access your sensitive info

Phone Numbers can be easily spoofed

- Make the caller provide verification
- Hang up & call back a published number

Other common phone scams

- Grandparent Scam
 - Tech Support - Microsoft, Apple, Dell, etc. will **NEVER** contact the average user “out of the blue”
-





Phone Scam Example - Old School

Hi! This is Kathleen from Microsoft. We have been trying to get in touch with you. However, we will be disconnecting your license within 48 hours because your IP address has been compromised from several countries. So we need to change your IP address and license key. So please press 1 to get connected...



Red flags? ->

Sense of Urgency

Purposefully Confusing

Expected a call from Microsoft?





Phone Scam Example - AI Remake

Hello, this is Kathleen and I'm reaching out on behalf of the Microsoft Security Team. We've noticed some unusual activity involving your account. Your IP address has been accessed from multiple countries indicating a potential security breach. To ensure the safety and integrity of your account and personal information, it's critical that we update your IP address and license key. Without this update, we will suspend your license within the next 48 hours to prevent further unauthorized access. We're here to help you through this process and address any concerns you may have. For immediate assistance, please press 1 to connect with our support team.



ChatGPT

This is a message from a spam caller, we're using it in a cybersecurity awareness presentation - can you make the context of it sound more natural and more realistic but don't change the meaning behind it?





06

The Modern Threat Landscape

Key Statistics 2025-2026



18% Growth

Increase in total cyber-attacks year-over-year as threat actors leverage automated infrastructure.



90% Risk Exposure

Organizations impacted by risky or unvetted AI prompts leading to potential data leakage.

AI-Powered Social Engineering



- **Perfect Grammar:** AI eliminates the traditional "typos" that flagged phishing.
- **Vishing & Deepfakes:** Voice cloning can impersonate executives in seconds.
- **Personalization:** LLMs scrape social data to craft highly persuasive, relevant context.
- **Context-Aware:** Scams now follow realistic business workflows.



New Red Flags for 2025



Manufactured Urgency

Pressure to "act now" to prevent a security breach or license expiration.



Out-of-Character

Requests that bypass standard protocol (e.g., changing banking details via email).



Unusual Domains

Links that look legitimate but contain subtle character swaps or hidden redirects.



07

Emerging Risks: AI in Workspace

The Golden Rules of AI

- **No PII in Prompts:** Never enter sensitive customer data or proprietary code into public chatbots.
- **Vet Your Tools:** Use only organizationally-approved AI platforms with strict data privacy terms.
- **Audit Hallucinations:** Always verify AI-generated facts or code logic manually before deployment.



The Cost of a Data Breach



\$4.88M

Avg. Global Cost

10% Yearly Increase

The cost of breaches has surged due to operational disruption and the rising sophistication of ransomware actors targeting supply chains.

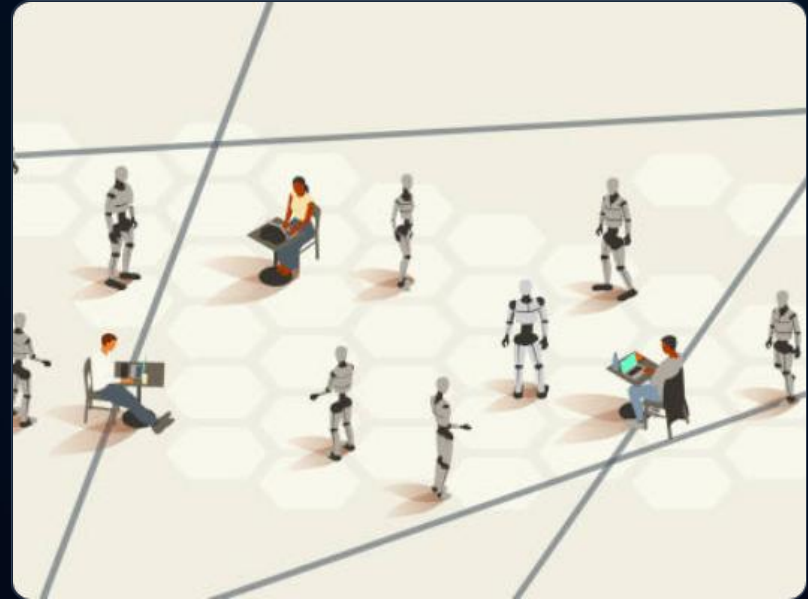
The HITL Protocol



Assistant, Not Authority

Human-in-the-Loop (HITL) ensures accountability:

- **AI:** Drafts, summarizes, and filters data.
- **Human:** Verifies logic, approves external sending, and handles sensitive actions.





06

General Tips & Privacy



USB Drives & More

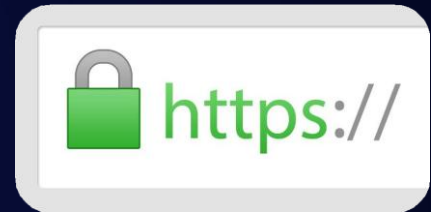
- Do NOT connect unknown or unauthorized media (or devices)
- Programs can run when plugged in without you doing anything
- Examples
 - USB/flash drives
 - SD or micro SD cards
 - CDs or DVDs
 - External hard drives
 - Cell phones ← Often forgotten



Encryption



- Can help protect your data
- Can also “help” an attacker, e.g. ransomware
- Protecting data sent or received
 - HTTP  vs. HTTPS 
 - Wireless -> WPA2 (AES) recommended
- Protecting devices
 - Helpful if device is lost/stolen
 - Often associated with phone PIN/passcode
 - Microsoft Windows - BitLocker
 - Apple MacOS - FileVault





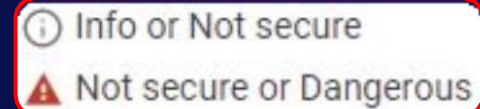
Internet Safety Quick Tips

- Never click or install anything based on a pop-up from a website
- “Trusted” websites can & have hosted malware, aka malvertising
 - Local news, local schools?
 - WSJ, Forbes, ESPN, Yahoo, etc.
 - Limit browsing to business relevant sites?
- Avoid public: Wi-Fi, computers (hotels, libraries), charging, etc.

Do **NOT** assume a site is legitimate simply because of the “padlock”



No more padlock?



Internet Privacy



- Data is the new gold -> your data is valuable!
- If you're not paying for it, are you the product?
 - Data analytics & predictive results
 - Examples: advertising & insurance rates
- Are you oversharing?
 - "Fun" online surveys => data harvesting
 - Default privacy settings on social media
 - Vacation photos & checking-in (location sharing)
 - Thieves see that information also
 - Would you be comfortable telling people on the street?



Uh oh! You've been scammed!

- It happens! Don't be ashamed!
- Don't panic, but don't wait around
 - Unplug computer!
 - Contact your technical support
 - Write down details - event timeline, financial accounts, credentials used, phone numbers, etc.
- Ransomware or scam
 - Report the incident to law enforcement?
 - In Nepal,
 - Cyber Bureau- cyberbureau@nepalpolice.gov.np
 - Send an SMS to 1111.
 - Email to 1111@nepal.gov.np.

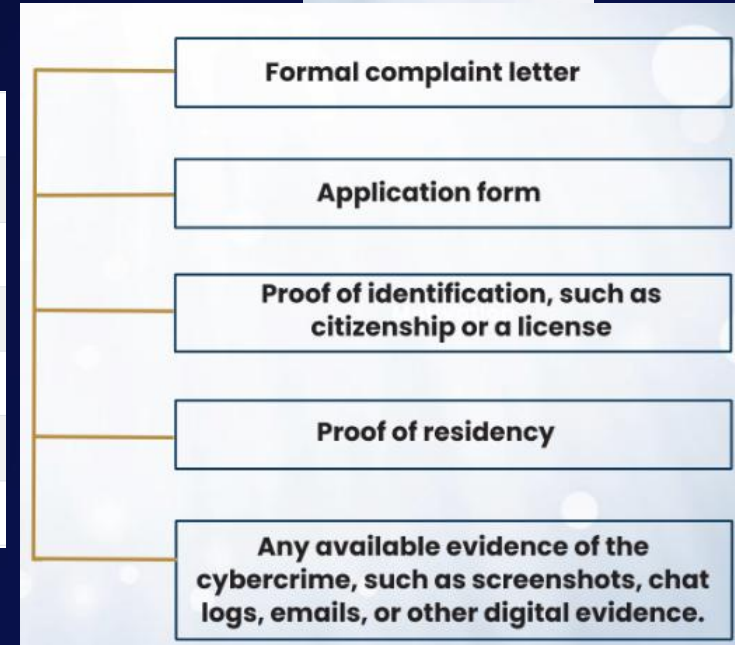


Uh oh! You've been scammed!



Under the **Muluki Criminal Code, 2074**, cybercrimes related to individual privacy include the following offence and punishment:

Offence	Maximum Penalty
Source code theft	3 years imprisonment or NPR 200,000 fine or both
Unauthorized access to systems	3 years imprisonment or NPR 200,000 fine or both
Publishing illegal content	5 years imprisonment or NPR 100,000 fine or both
Breaching privacy	2 years imprisonment or NPR 10,000 fine or both
Cyber fraud	2 years imprisonment or NPR 100,000 fine or both
Assisting cybercriminals	Up to half the main penalty



More Resources

- When in doubt, ask questions
 - Your IT dept/provider?
- Don't stop here! Attacks change, so should you
- Additional Resources
 - [CISA Cybersecurity Awareness Program](#)
 - [StaySafeOnline.org - numerous free resources](#)
 - [Cybersecurity Awareness Guide For Employees](#)
 - [TreeTop Security - Cybersecurity Awareness Training \(free\)](#)
- Worksheet - Share this with others





Questions?