

# Security Awareness Training 2023



# Secure the Remote Workplace

---



**Secure Technology**








26C016 16C010108A



**User Behavior**

026L R6U9A10L



- 01 Router username and password (strong password)** 
- 02 Automatic updates (unpatched vulnerabilities)** 
- 03 Connect with the company VPN** 
- 04 Utilize multi-factor authentication** 
- 05 Download or install confirmed software (impersonating legitimate apps)** 
- 06 Report suspicious activity (phishing or unexpected email, high resource usage)** 
- 07 Password manager** 



01

**Do not leave your device unattended (Install malware, scan photos or documents)**

02

**Keep your work separate (Prevent shoulder surfing, separate guest access )**

03

**Secure video meeting**

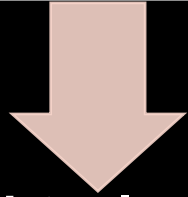
04

**Do not lend or borrow anyone's device**

05

**Immediately report missed or stolen IT equipment**

Public Wi-Fi is a significant risk to an individual's privacy.



Utilize a virtual private network (VPN) to reduce the risk

Use HTTPS

Avoid accessing high-sensitive information

Turn off file sharing

Turn off auto-connect to public Wi-Fi networks

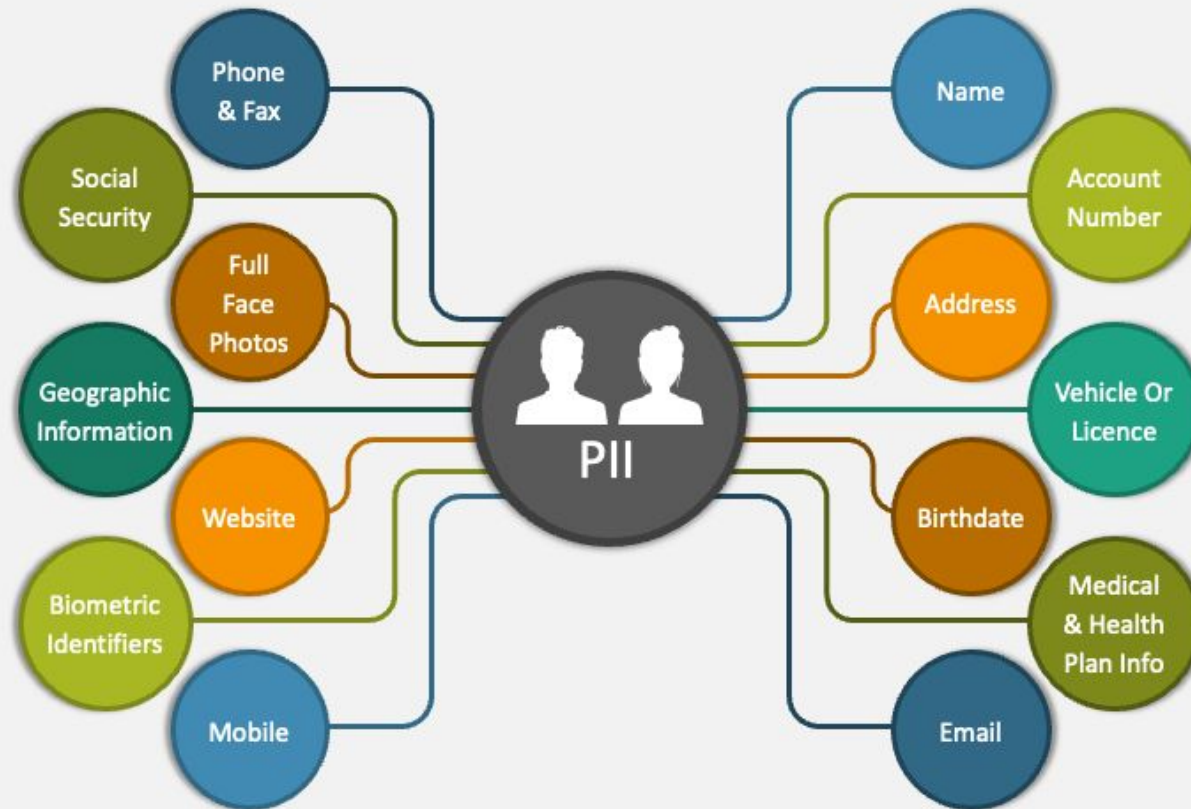


# Security Awareness Training 2023

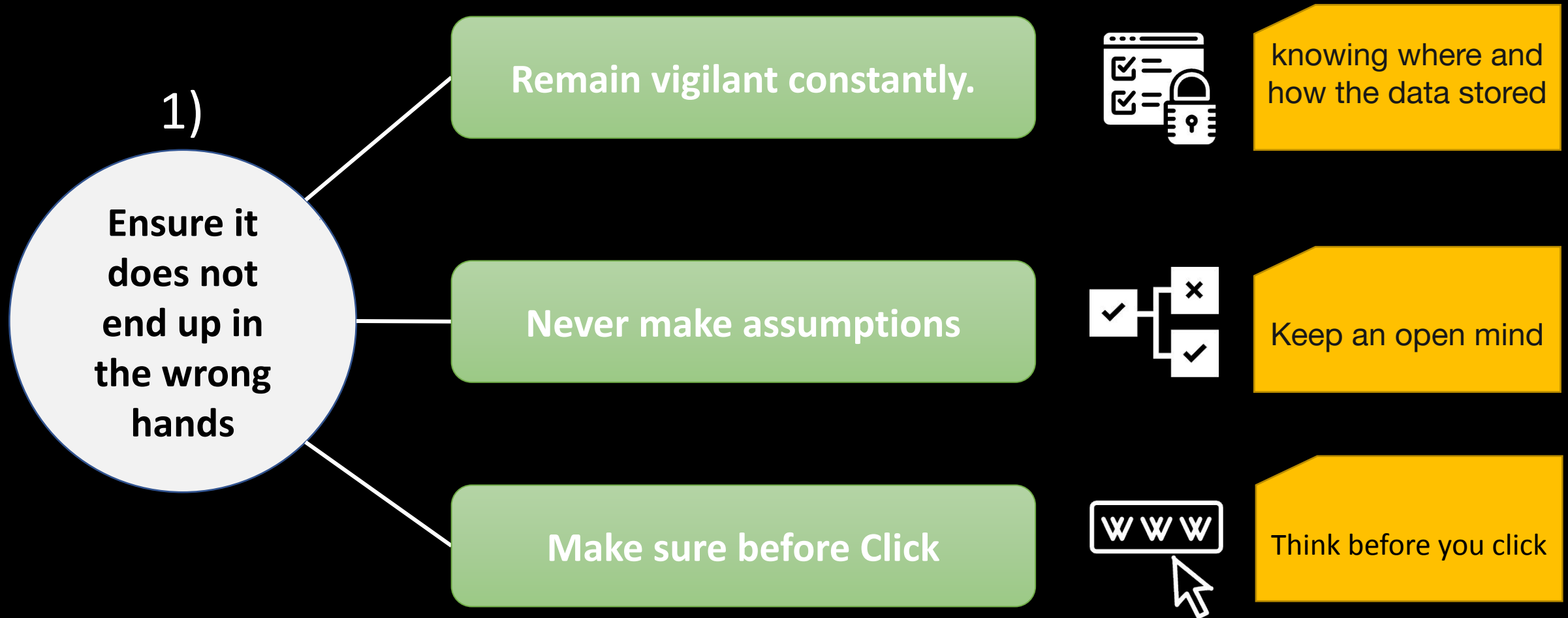


# What is PII?

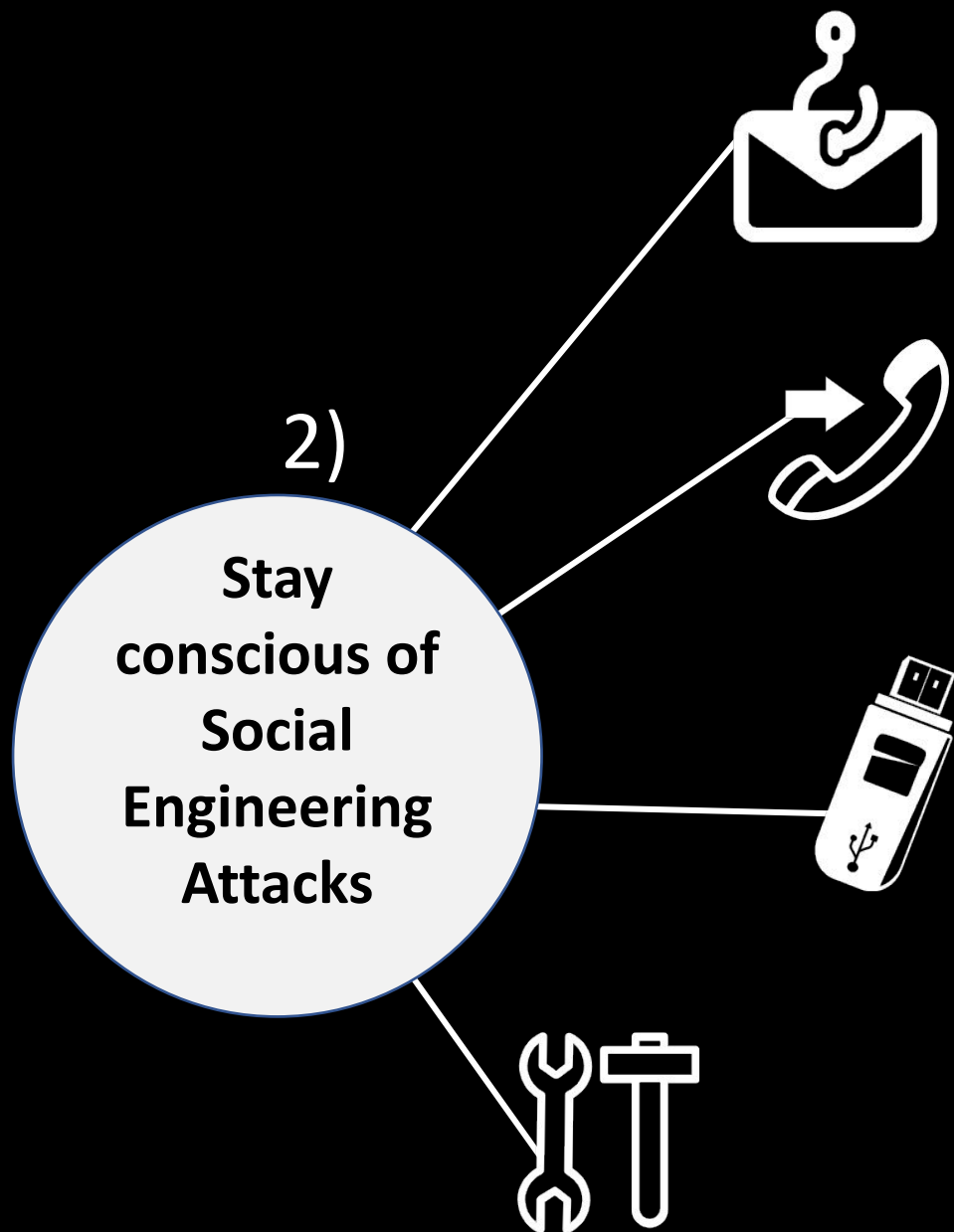
## PERSONALLY IDENTIFIABLE INFORMATION (PII)



# How to Protect PII







# PHISHING



**Report anything unusual**

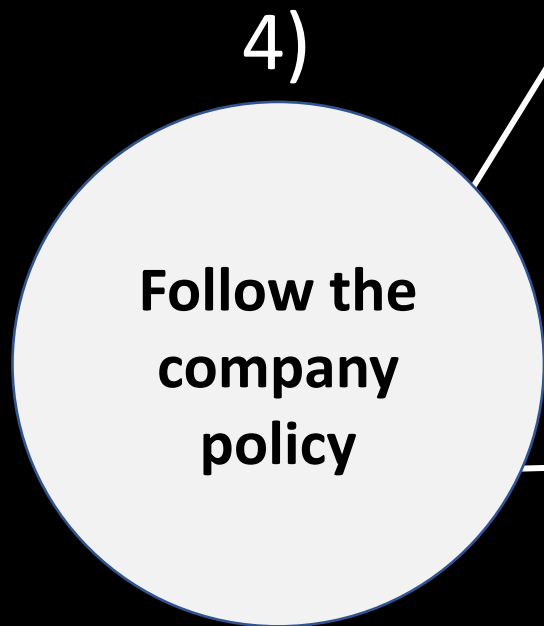
3)

**Correct data  
to  
Correct person**

The document has the required details and nothing beyond what the partner requires.

You refrain from mistakenly sending it to the incorrect individual.

**double-check the recipient**



**Data lifecycle management**

**Data access management**

**Who has  
access and  
why**



**Please make sure you comply with the company policy.**



# Security Awareness Training 2023



# Do you know the most successful Cybercrime Strategies?

DoS or DDoS

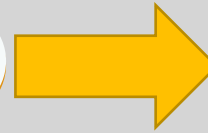
Malware

Phishing

Ransomware

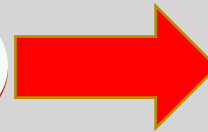


01



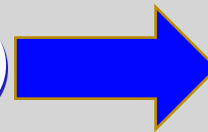
Roughly **15 billion** spam emails make their way across the internet every day

02



Roughly **90 of data breaches** occur on account of phishing. According to the US Federal Bureau of Investigation, phishing attacks may increase by as much as **400% year-over-year**.

03



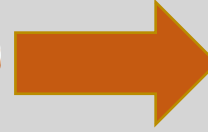
Roughly **65% of cyber attackers** have leveraged spear phishing emails as a primary attack vector.

04



**84% of US-based organizations** state that security awareness training has lowered phishing failure rates.

05



Even with **robust security mechanisms** in place, such as firewalls, antivirus software, and intrusion detection systems, phishing attacks can still **succeed** if a **user** falls for the scam

# Phishing Stages



01

Check the sender's email address

02

Look for urgent or threatening language

03

Check for spelling and grammatical errors

04

Avoid clicking on links  
(hover the mouse over the link)

05

Check for a secure connection

06

Beware of attachments

07

Verify with the sender

**From:** domain@domain-name.com

**To:** Your email

**Subject:** Apple Facetime Information Disclosure



National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

**Facetime Verification**

<http://www.udeledu.net/1/?login.htm>

This website will be available for 72 hours.

National Security Department



## Example 4

**From:** Microsoft office365 Team [mailto:cyh11241@lausd.net]  
**Sent:** Monday, September 25, 2017 1:39 PM  
**To:**  
**Subject:** Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

Microsoft Security Assistant  
Microsoft office365 Team! ©2017 All Rights Reserved

<https://x.co/f4zbq4u/?=<email>%3hdo>  
Click or tap to follow link.

**From:** Microsoft office365 Team [mailto:cyh11241@lausd.net]  
**Sent:** Monday, September 25, 2017 1:39 PM  
**To:**  
**Subject:** Your Mailbox Will Shutdown Verify Your Account

1 Suspicious email address.

2 Threatening language.



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

3 Threatening language.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

4 Suspicious link.

Microsoft Security Assistant  
Microsoft office365 Team! ©2017 All Rights Reserved

5 Odd capitalization and punctuation.

# Step 8

# VirusTotal

http://paypal1.com/

Did you intend to search across the file corpus instead? [Click here](#)

7 / 90

7 security vendors flagged this URL as malicious

http://paypal1.com/  
paypal1.com

200 Status  
2023-02-17 02:00:09 UTC  
1 month ago

multiple-redirects

Community Score

DETECTION DETAILS LINKS COMMUNITY 3

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ Do you want to automate checks?

alphaMountain.ai	Phishing	Avira	Phishing
BitDefender	Phishing	Fortinet	Phishing
G-Data	Phishing	Seclookup	Malicious
Sophos	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	Bfore.AI PreCrime	Clean
BlockList	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	CyberCrime	Clean

# Security Awareness Training 2023



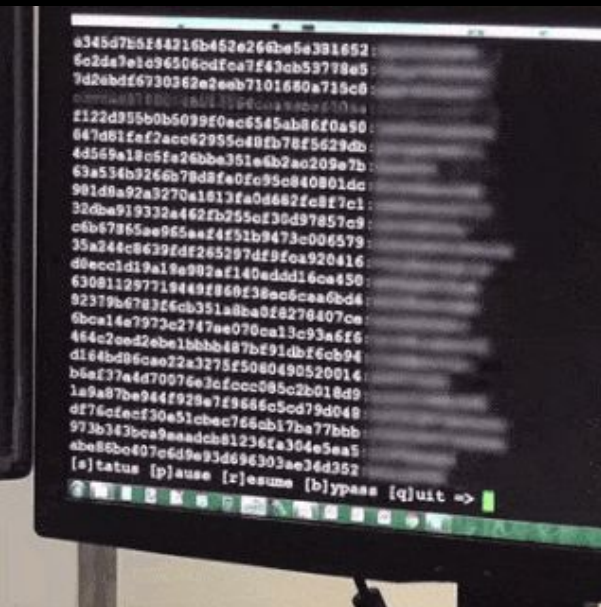
01

How long  
would it take to  
crack  
an 8-character  
password?

02

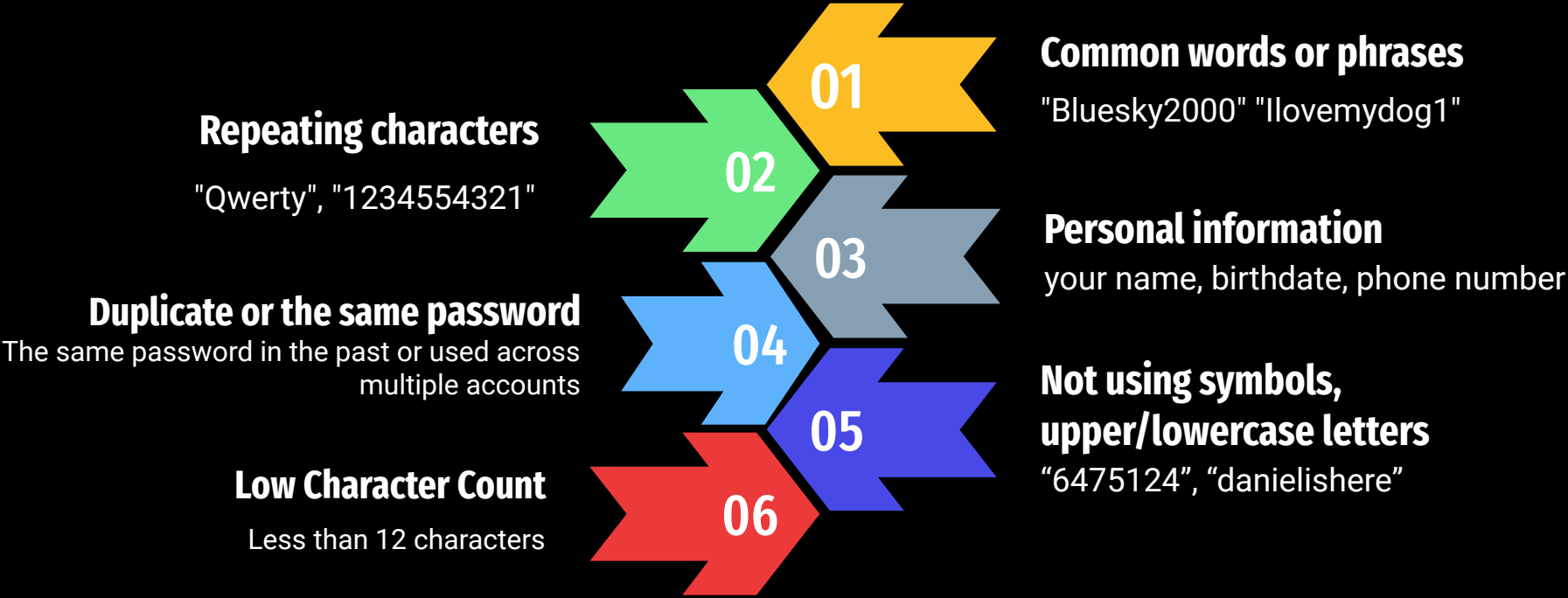
How long  
would it take to  
crack  
a 12-character  
password?

NUMBER OF CHARACTERS	NUMBERS ONLY	UPPER OR LOWERCASE LETTERS	UPPER OR LOWERCASE LETTERS MIXED	NUMBERS, UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS, SYMBOLS
3	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
4	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
5	INSTANTLY	INSTANTLY	INSTANTLY	3 SECS	10 SECS
6	INSTANTLY	INSTANTLY	8 SECS	3 MINS	13 MINS
7	INSTANTLY	INSTANTLY	5 MINS	3 HOURS	17 HOURS
8	INSTANTLY	13 MINS	3 HOURS	10 DAYS	57 DAYS
9	4 SECS	6 HOURS	4 DAYS	1 YEAR	12 YEARS
10	40 SECS	6 DAYS	169 DAYS	106 YEARS	928 YEARS
11	6 MINS	169 DAYS	16 YEARS	6K YEARS	71K YEARS
12	1 HOUR	12 YEARS	600 YEARS	108K YEARS	5M YEARS
13	11 HOURS	314 YEARS	21K YEARS	25M YEARS	423M YEARS
14	4 DAYS	8K YEARS	778K YEARS	1BN YEARS	5BN YEARS
15	46 DAYS	212K YEARS	28M YEARS	97BN YEARS	2TN YEARS
16	1 YEAR	512M YEARS	1BN YEARS	6TN YEARS	193TN YEARS
17	12 YEARS	143M YEARS	36BN YEARS	374TN YEARS	14QD YEARS
18	126 YEARS	3BN YEARS	1TN YEARS	23QD YEARS	1QT YEARS



# Secure Password

## Avoid Weak Passwords





Best Practice: Password Security



Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

01

At least 16 characters

02

Combination of upper and lowercase letters, numbers, and symbols

03

Consider unique password for each account

04

Use an approved password manager to securely store your passwords.

05

Use an account lockout policy & Change the password (30/60/90 day)

e.g. = EpbGan#QFo741Xg&svFbS OR PHRASE  
My-Company/Paid-for-my-house-5764

# Password Manager



**Set a master password with 20 characters including upper and lowercase letters, numbers, and symbols**

**Generate a random password for each account that has 20+ characters in length and combination of upper and lowercase letters, numbers, and symbols**

**Save along with the related URL**

# Agenda

## Security Awareness Training 2023





# How can I ensure safer operation while living or working in a digital environment?

The internet was not initially built with security in mind

The internet is constantly changing

Failure to protect yourself in web browsing might result in the spread of malware or viruses to other users and networks, which can have wider-reaching impacts.



# Common web browser attacks:



01

## Intercepting Communication

Using an insecure public network or browsing on HTTP can allow attackers to see passwords + PII in the clear.



02

## Browser Extension Exploits

Malicious extensions can steal data, inject ads, or redirect users to malicious websites.



03

## Session Hijacking

As an example, this is typically done when a malicious actor is tempting you to click on a link with a session ID in a FB comment.

# Two-factor Authentication

Enable two-factor authentication for your online accounts whenever possible. This adds an extra layer of security by requiring a second form of verification in addition to your password.

## Password Manager

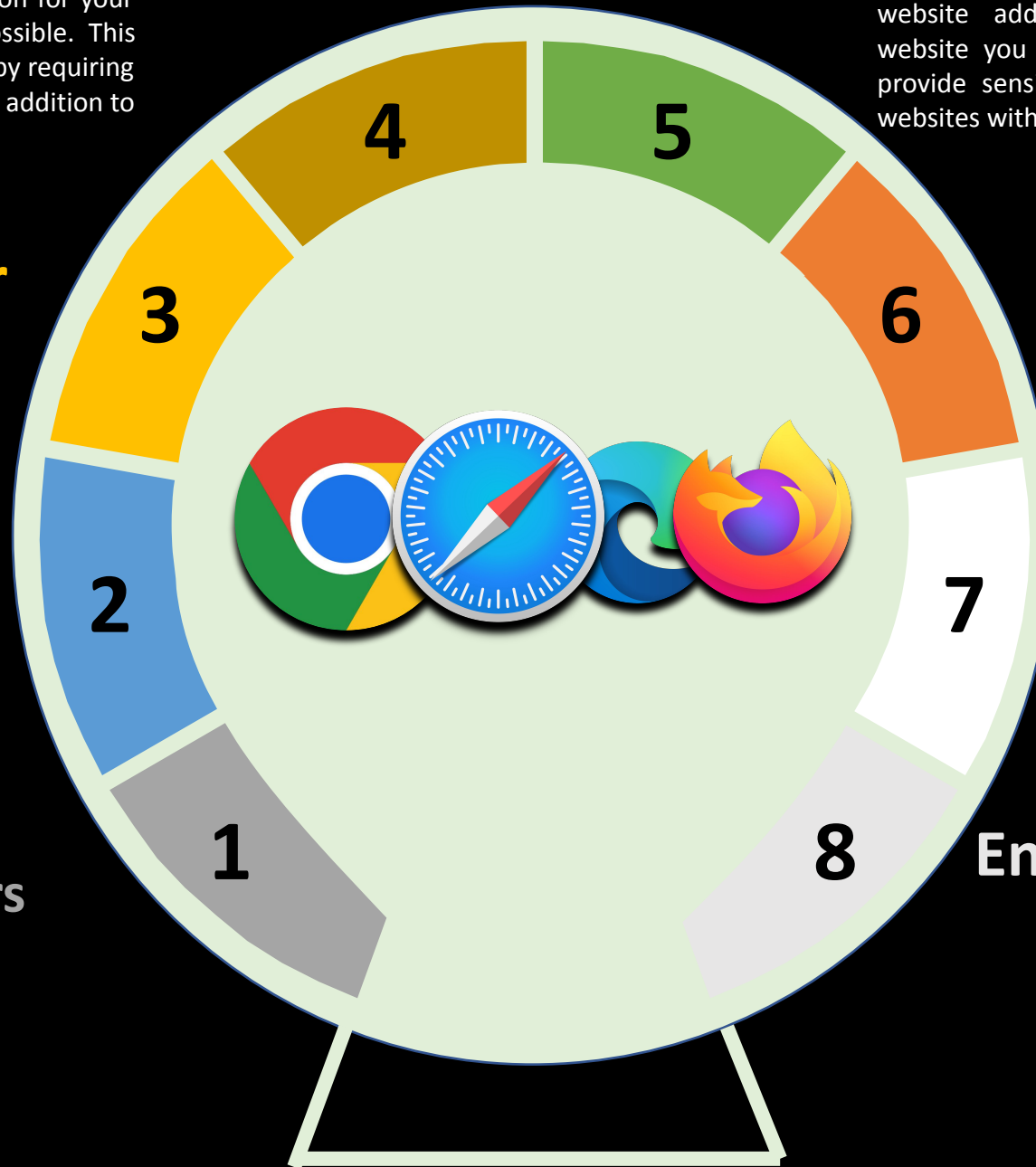
Use a password manager to generate and store your passwords. Do not save your passwords in the browsers.

## Strong Passwords

Use strong passwords for all your online accounts, and avoid using the same password for multiple accounts.

## Trusted Web Browsers

Use a well-known and reputable web browser like Google Chrome, Mozilla Firefox, or Apple Safari



## HTTPS

Look for a lock icon or "https" in the website address to ensure that the website you are visiting is secure. Only provide sensitive information on secure websites with an HTTPS connection.

## Download

Only download software and files from reputable sources, and be careful downloading anything that seems too good to be true.

## Update Software

Keep your operating system, web browser, and other software updated with the latest security patches.

## Enable Browser Security

Enable browser security settings such as pop-up blockers, anti-tracking features, and the "Do Not Track" option to protect your privacy. Only use browser extensions and plugins that you trust and need. Many malicious extensions and plugins can compromise your security and privacy.

# Agenda

## Security Awareness Training 2023







**MFA is a method of confirming or authenticating an individual's identity through the use of two or more verification steps.**



**MFA can be bypassed through social engineering tactics, such as phishing attacks or impersonation, it is still much more difficult for a hacker to breach than single-factor authentication**

### **One-Time Password (OTP)**

A one-time authorization code, passphrase, or sending pin as an email, text message, or through an authentication app.



### **Biometric Identifiers**

An identifier that uses facial recognition, fingerprint scans, or speech patterns to verify users



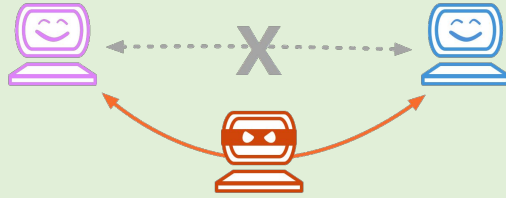
### **Tokens or Smartcard**

A physical <sup>S</sup>item used to access an account that must be used in conjunction with other identifiers like usernames, passwords, and pins.



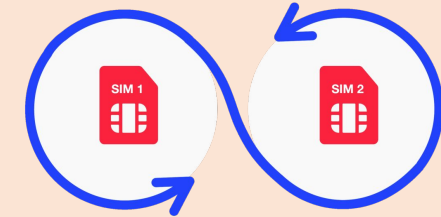
### Man-in-the-Middle Attack

refers to the act of a cybercriminal positioning themselves between a potential victim and a legitimate service, such as the victim's banking website, with the goal of accessing their credentials and other valuable information



### SIM Swap

A SIM Swap is when your phone number and other related information are transferred to another phone



### SMS Rogue Recovery

The goal is to trick victims into eventually giving them an MFA code that will give them access to the user's account, like a bank account.



# Security Awareness Training 2023



## PHISHING EMAIL

It's important to be cautious when receiving emails from unknown or suspicious sources, and to never click on links or download attachments unless you're sure they're safe.



## Important types of attack targeting corporate users

## QR SCAM

A QR code scam is a type of fraud that involves the use of QR codes to trick victims into revealing personal information or downloading malware onto their devices.



- In a typical QR code scam, the attacker creates a QR code that appears to be legitimate, such as a code that directs the user to a website or a promotional offer. However, when the victim scans the QR code with their smartphone or other devices, they are taken to a malicious website or app instead.

## FAKE MEETING REQUEST

A fake meeting request can be particularly effective because it appears to be a normal part of the recipient's work routine and may not raise suspicion until it's too late.



- Required to download additional files e.g., Software Update

## LINKEDIN PHISHING

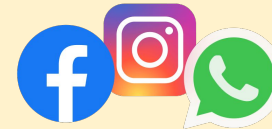
An attack using LinkedIn is a type of social engineering attack where cybercriminals use the LinkedIn platform to trick users into revealing sensitive information or downloading malware onto their devices.



- fake job offers
- invitations to connect with unknown individuals
- or messages claiming to be from trusted contacts.
- In some cases, attackers may create fake LinkedIn profiles that look like legitimate ones to gain the trust of their targets

## SOCIAL MEDIA ATTACK

An attack using LinkedIn is a type of social engineering attack where cybercriminals use the LinkedIn platform to trick users into revealing sensitive information or downloading malware onto their devices.



- Phishing
- Fake profiles
- Malware distribution
- Account takeover
- Clickjacking



# How to protect ourselves?



**your actions impact your organization's safety**



**Embed cybersecurity as a culture**



**Use knowledge and best practices gained here to defend the team**

## Human Firewall

