

End User Security Awareness Training

Presenter name – Khaing Linn Htun

Date – 24 / 5 / 2024



Our Focus



Using strong passwords and a password manager



Enabling multi-factor authentication

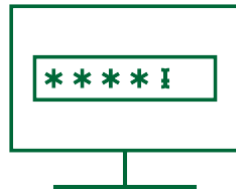


Recognizing and reporting phishing



Updating software

■ Passwords: Keys to Your Digital Castle



Long

At least 12 characters
in length



Unique

Never reuse
passwords



Complex

Combination of
character types

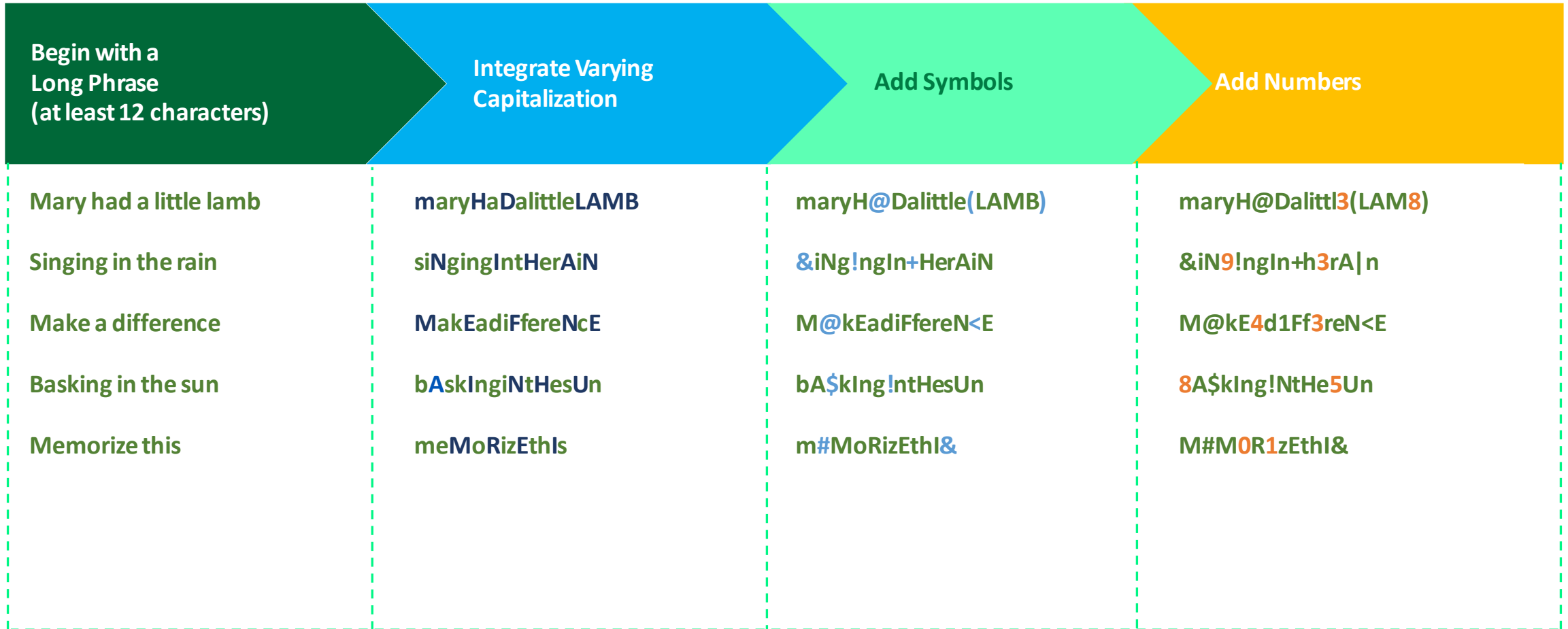
20 Most Common Passwords of 2024

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	111111	12345678	12345678	16	1234	password1	666666
7	123123	111111	111111	17	iloveyou	1234	123321
8	12345	123123	12345	18	aaron431	qwertyuiop	654321
9	1234567890	1234567890	col123456	19	password1	123321	777777
10	senha	1234567	123123	20	qqww1122	password123	123

Watching you by
hacker



Creating Long and Complex Passwords



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)

- Microsoft Edge
- Chrome?

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 length <-> time to crack

Time for an attacker to brute force passwords.

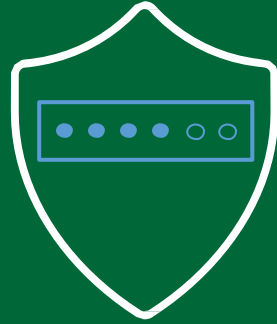
Are you in the yellow or green?

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	Instant	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

Enabling Multi-Factor Authentication



Microsoft authenticator



Something You Know

- Password
- PIN
- Passcode
- Pattern



Something You Have

- Authentication code via text/email/phone/token
- Verification request from a mobile app
- USB plugged into the device attempting to access the account
- Smart card or keys



Something You Are

- Fingerprint scan
- Facial recognition
- Retina scan
- Voice verification

passwords exposed

24 Billion

passwords exposed by hackers in 2022

2FA - two-factor auth

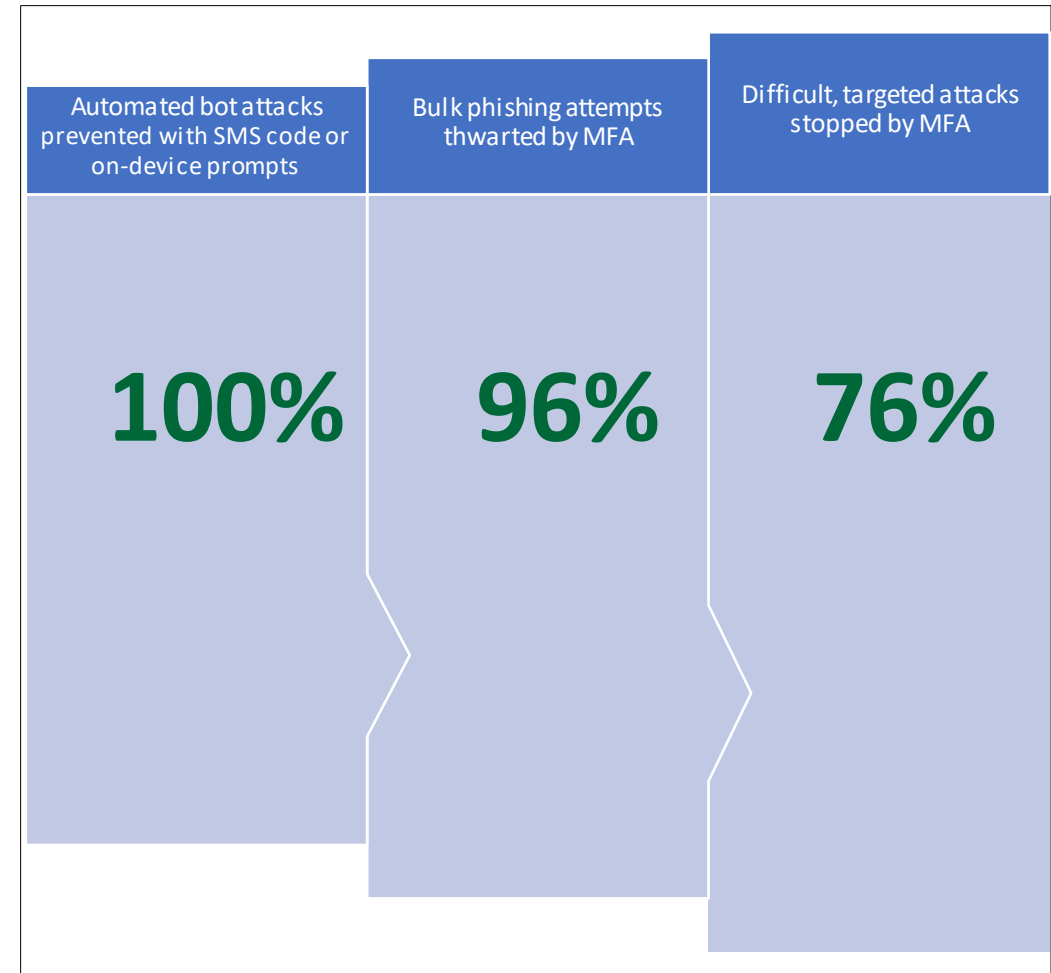
What is 2FA?

- “Beyond” a username and password
- Second form to prove it is you
- Typically, out-of-band

“Your one-time code is...”

- SMS (Not as Secure)
- Phone call (Not as Secure)
- Applications
- Email
- Phone pop-up
 - Google Authenticator
 - Microsoft Authenticator

MFA Success Stories



Tips, Best Practices and Considerations

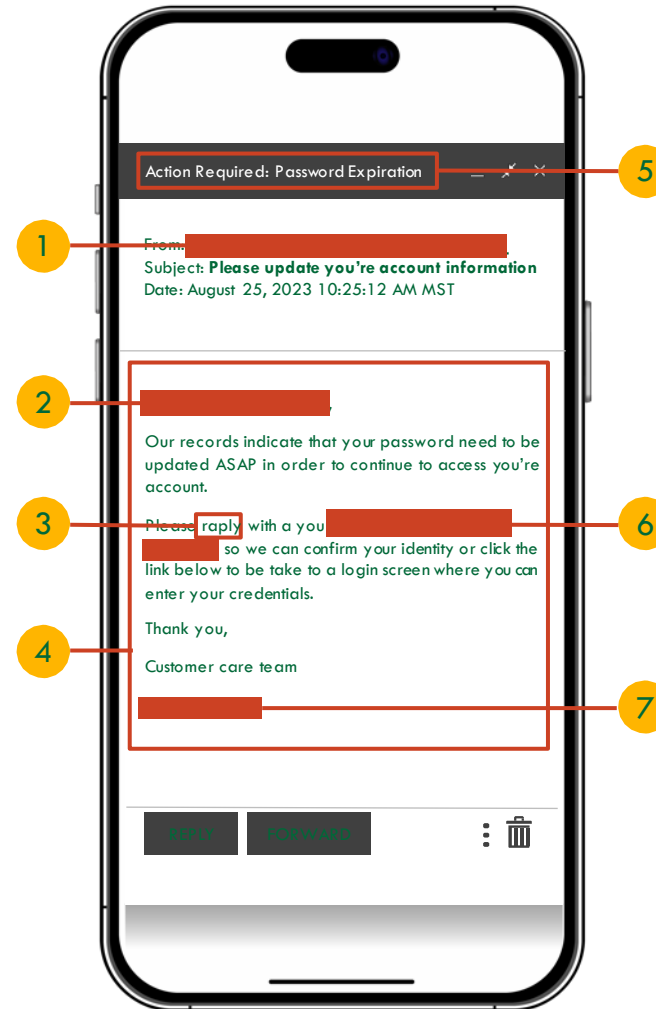
Availability	Prioritization	Diligence
<p data-bbox="122 378 494 444">Not every account or device offers MFA.</p> <ul data-bbox="173 464 749 572" style="list-style-type: none">• Stay abreast of security updates that may enable the functionality <p data-bbox="122 646 687 675">Common types of accounts that offer MFA:</p> <ul data-bbox="173 698 529 935" style="list-style-type: none">• Banking / Credit Card• Insurance / Medical• Email• Social Media• Stores / Online Shopping	<ul data-bbox="873 464 1154 601" style="list-style-type: none">• Financial• Health• Personal Contacts	<p data-bbox="1587 378 2160 444">Continue to use long, unique, and complex passwords.</p> <ul data-bbox="1638 464 2219 535" style="list-style-type: none">• Update your password if you are aware of potential compromise <p data-bbox="1587 609 2040 675">If you receive multiple illegitimate MFA requests:</p> <ul data-bbox="1638 698 2237 872" style="list-style-type: none">• Do not approve requests!• Contact the service or platform and alert IT immediately• Change your password for the account

| Recognizing and Reporting Phishing

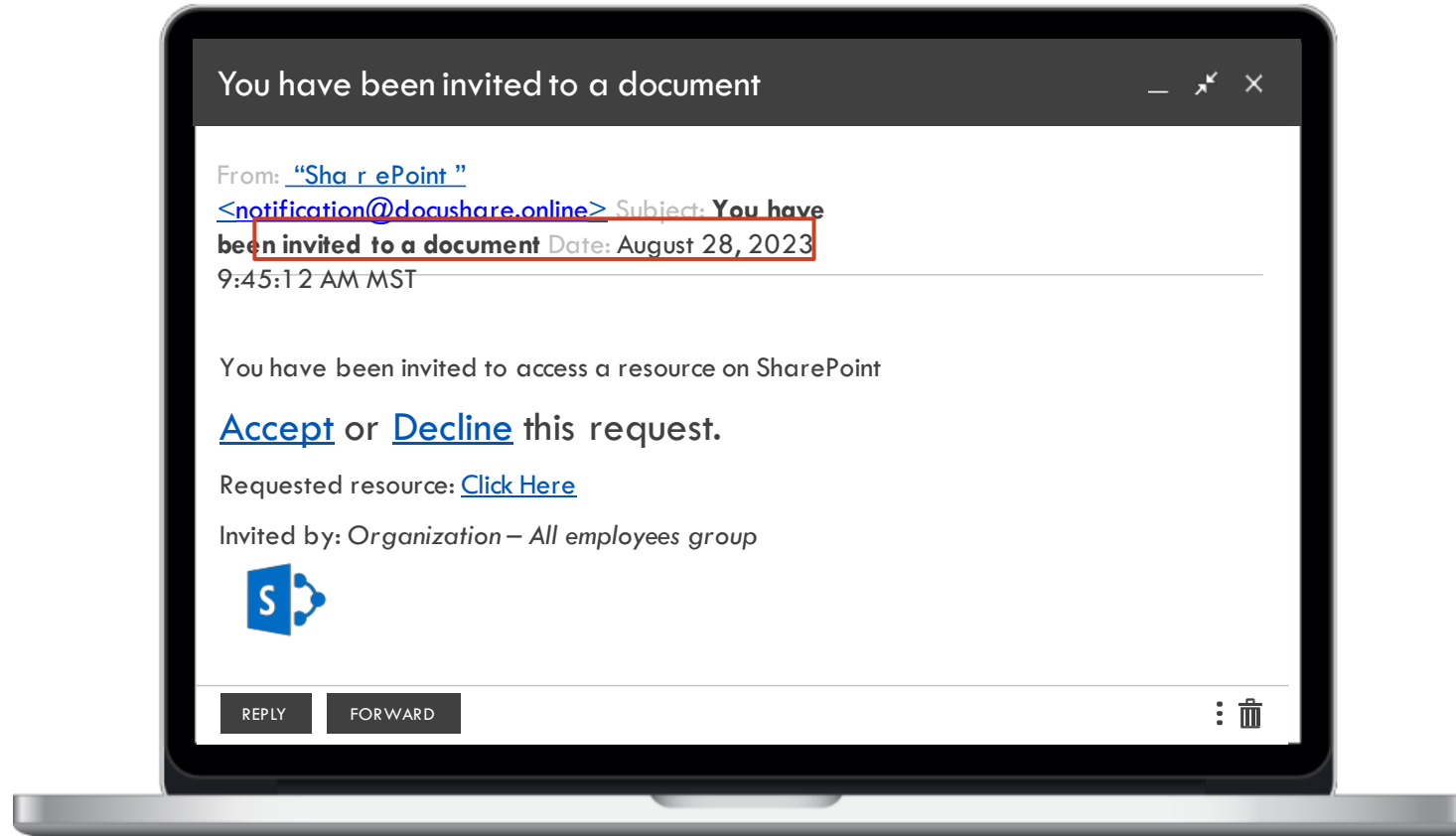


Phishing

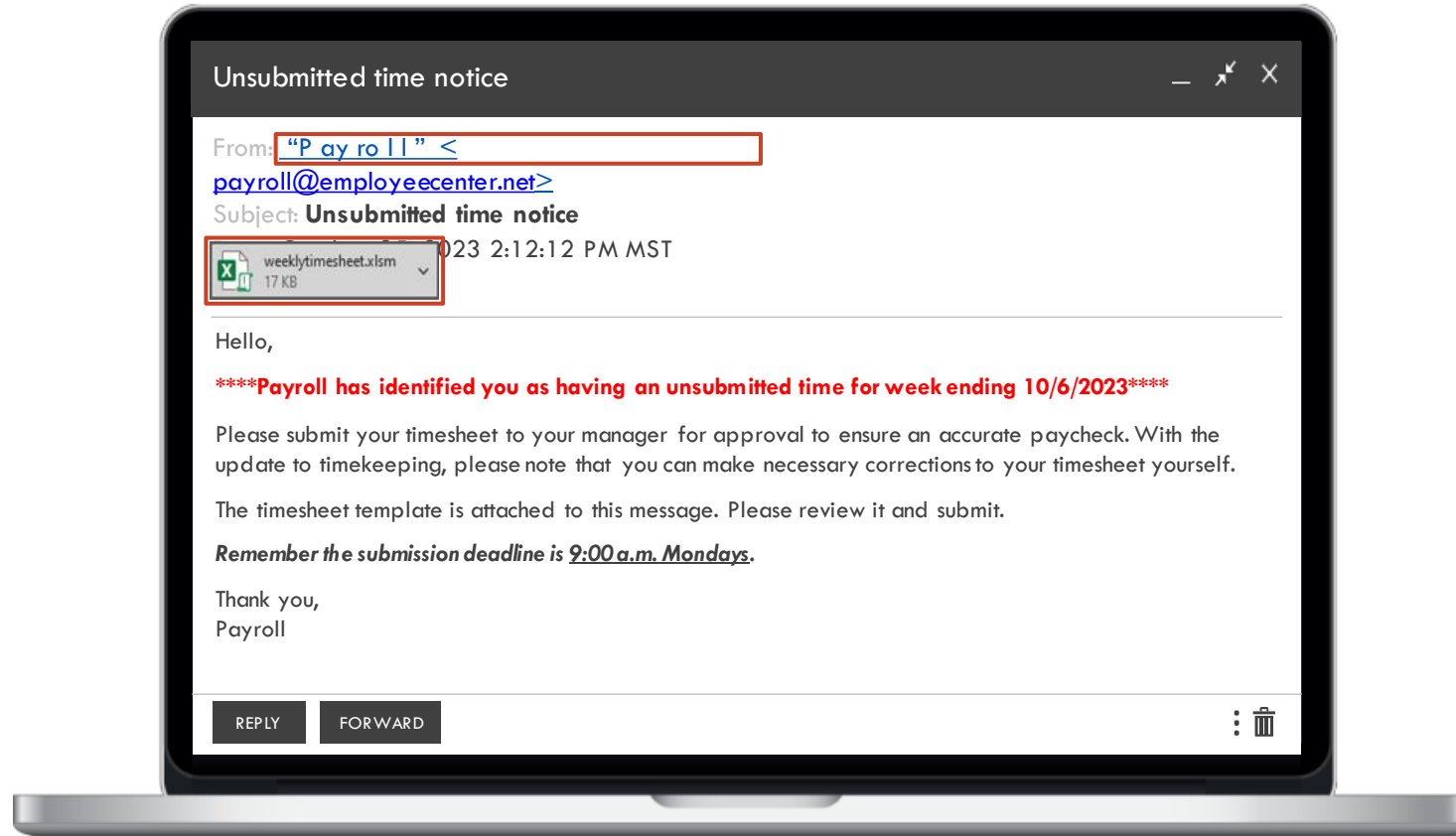
- 1 Unofficial or unfamiliar sender address
- 2 Generic greeting
- 3 Misspelled words and grammatical errors
- 4 Unprofessional or atypical formatting
- 5 Language intends to urge immediate action
- 6 Unusual request for sensitive information
- 7 Links that are shortened or mask the destination



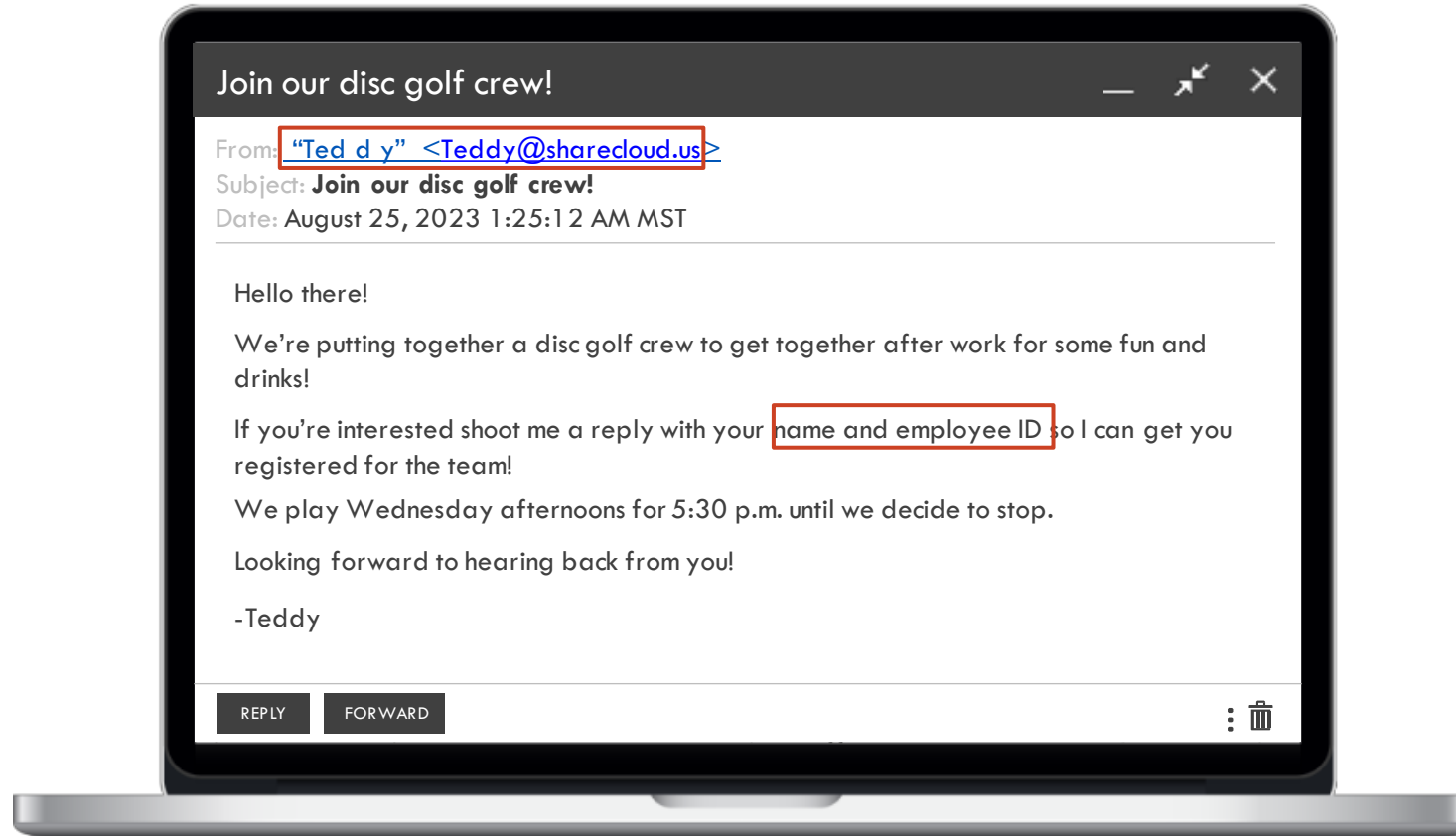
Sophisticated Phishing



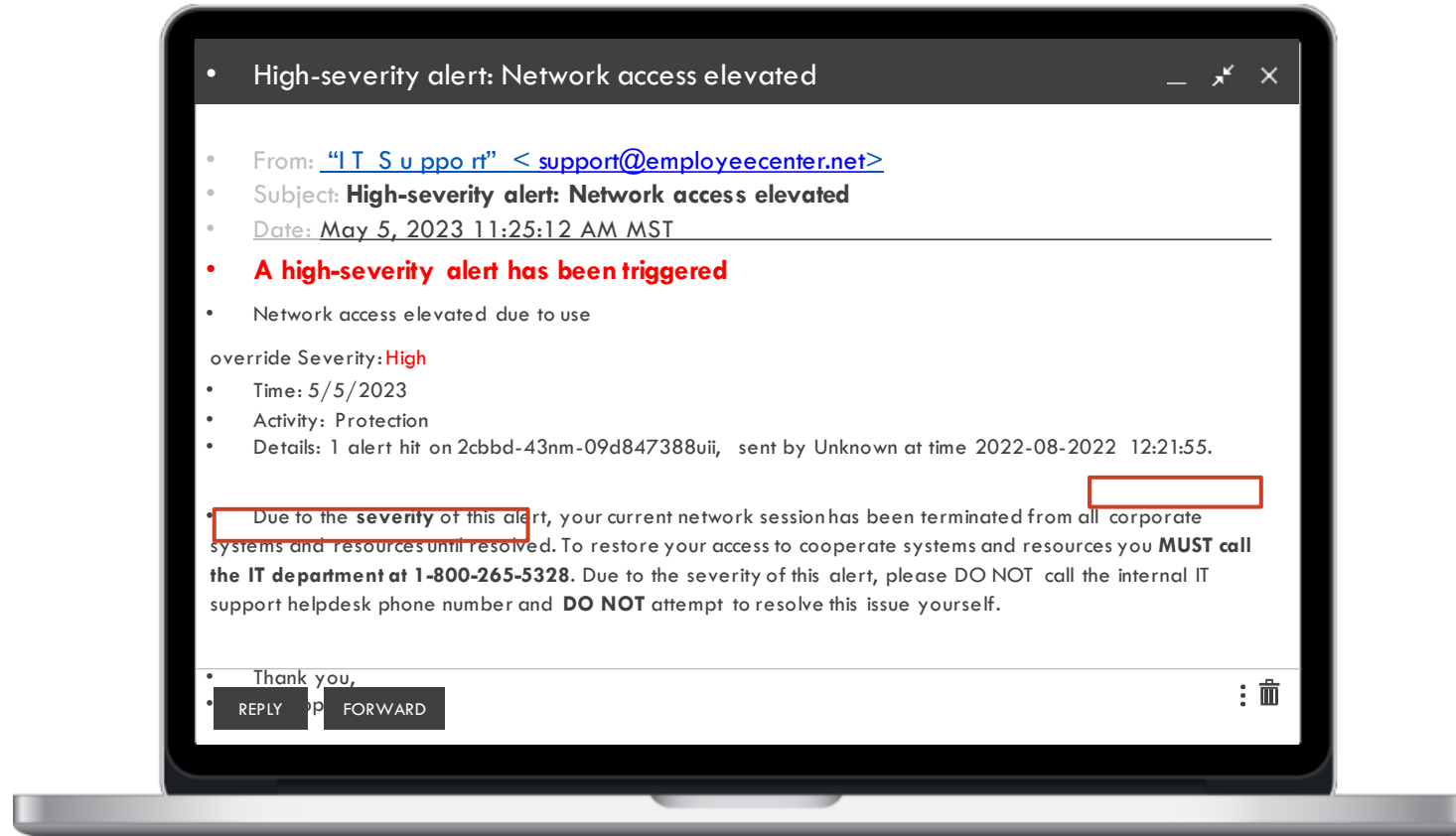
Phishing Attachments



Phishing For Replies

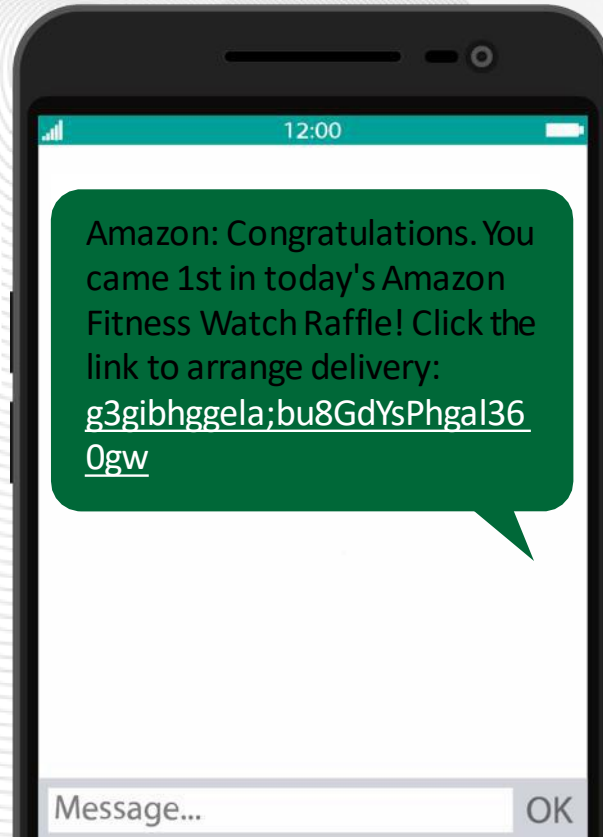


Coordinated Attack



Smishing Examples

I found this old pic of us!
What year was
this? <http://tinyurl.com/84692tjk>



Google Security: Changes were recently made to your Google account. [Log in](#) to configure your settings.

Unusual activity detected in your online banking. Please log in at <http://bit.do/dg2Q> to secure your account.

When You Catch a Phish

What to do when you suspect a message is phishing



Anywhere

- Do not click interactive elements in the message
- Do not reply to or forward the email
- Do not click, open or download attached files
- Do not follow the message's instructions
- Notify the purported sender using a new email or alternate method
- When authenticity is not established, delete the message immediately



At Work

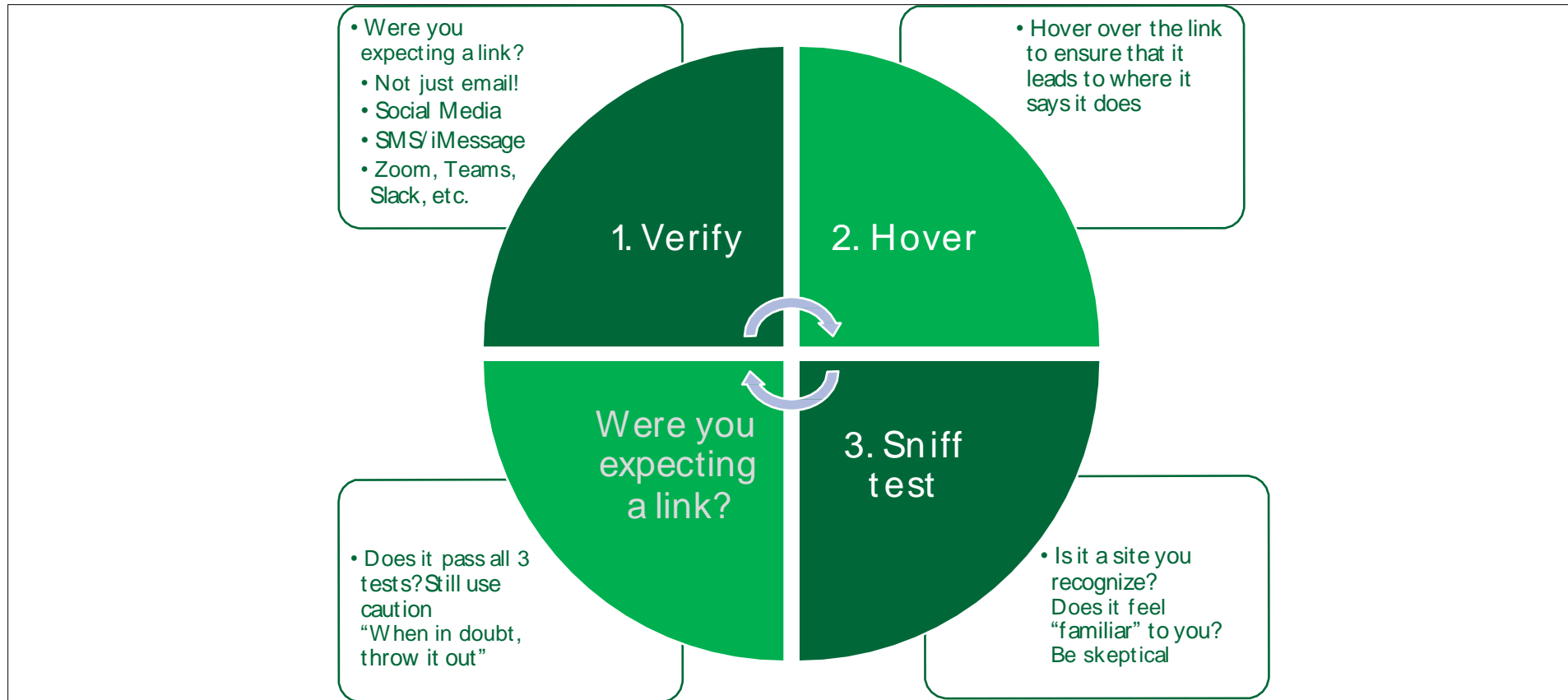
Follow your organization's policy, which may include reporting it to your technical support team



At Home

- Report the message to the purported sender and, if possible, the email provider
- Block the sender's email address or phone number

Is the link safe in 4 steps



Link expander

www.linkexpander.com

Other Email Scams

Everything is allowed! Just don't forget Via.gra.

 BEST CAN DRUGS <onhne_p\$1\$1'opShfal-pharmacy.canada >

To:

SHIP NQW [RX.COMPANYJ

First Name: [REDACTED]
S/n: Tuf*.d.y. M left J8, .)017 1::ll
P0t
Subject: INSTRUCTION FOR 'LMRFRANSIFR

Hi [REDACTED]

I need (f) to process a wire transfer to a ne"Y ...1!..-dow
please come (, ... 11'hell) ou call 'ge'
cta.le

Dear Apple Customer,

To 9tl IND lruo IOOJ apple coum. yoo11ntod 10 conffmlll your kccoom . ll's usy: Cldc
tilt link //4bit to Ollm a ucurl t>'OMt l'riidow. c f\rm thw.l ,ou'rt dlF OW'nt of tnt
account and cIM follow tht iMtructkms.

The lank lri (xl)ire 72 lOllts ttr t h i s w l!
stilt.

[Unlock"- "IM I\(\) >](#)

ICCOU) .rl .-n & DN(Cim <817ti1068ltn xmitmxLinfo>
l.&nill9 MI.
COU11 Oit'



Customer Support

Hello Dear Customer!

W.IIMII .c. d - .)' O u t - SoP1NMUjCiOM)Out -
. n t . . (ou do ICCU1)ON 'FOUI-III.. 2* ,..._ 01*1"9 tllt
oecea.tr ci<LMllcd

[Update Now](#)

<http://redirect.kereskedj.com>

W.fiOoOIMio-.....e v - -
Amazon.com

 : fJ lld'
Subject: [REDACTED] Memo


... has shared

[Memo.pdf](#)

[Open](#)

...
)t

..... c J

 Tuesday, 28 January 2020 at 03:51
[Show Details](#)

G o Ifltmc.hed rfocumtnt on Qfety mus Jrti r th f 1 tilts p r t of awQN'liM.
1M thWm t | Qllsrrtyou.

1MtheI btlow to download

[Safety Measures.pdf](#)

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

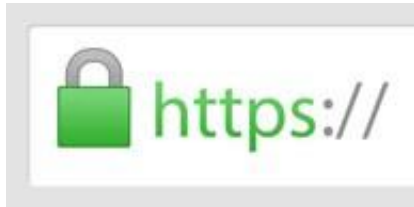
Regards
Dr [REDACTED]
Specialist wuhan-virus-advisory

General Tips & Privacy



- 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?

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?

ⓘ Info or Not secure
⚠ Not secure or Dangerous

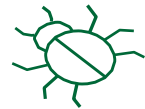
Enable updates straight from the source



Automation: Enable **updates straight from the source**



Be suspicious of pop-up windows that urgently demand software updates via download.



Avoid pirated and unlicensed software, as they often serve as a tool to spread malware.

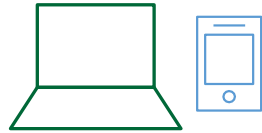


Do not click **links in emails pushing for application, software or device updates**.
Navigate directly to the source and check for updates.

Key Cybersecurity Behaviors



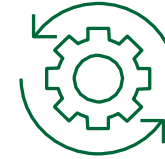
Use Strong Passwords



Enable MFA



Recognize and Report
Phishing



Update Software

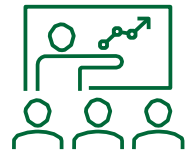


Regularly Assess Your
Digital Hygiene

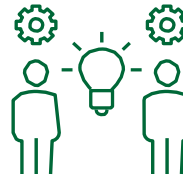
To stay safe online, make these behaviors part of your regular routine



Create Backups



Learn From Security
Awareness Training



Share Cybersecurity
Knowledge With Others



Avoid Using Public WiFi



Use a VPN

Thank You...

