PRIVACY REF

Effective operational privacy

Best Practices for Remote Working in a Government Environment

Bob Siegel
President, Privacy Ref
Fellow of Information Privacy
CIPP /US/G/C/E, CIPM, CIPT

Florida Government Finance Officers Association

Bob Siegel

Founder and President of Privacy Ref, Inc.

- Previously, Staples Sr. Manager of Privacy and Compliance

Fellow of Information Privacy awarded by the IAPP

- Certified Information Privacy Professional
  - US Private Sector Law
  - US Government Privacy Law
  - European Data Protection
  - Canadian Data Privacy Law
- Certified Information Privacy Manager
- Certified Information Privacy Technologist

Facilitator for IAPP Privacy Courses

PRIVACY REF

AGENDA

Florida Government Finance Officers Association

Why work remotely?

Organizational considerations

- Creating a “work remotely” policy
- Securing your computer
- Protecting your network connection
- Establishing strong passwords
- Tips for using your mobile devices
- Handling confidential papers

Personal considerations

- Setting up a home workspace
- Guarding against scams
- Protecting your personal information

PRIVACY REF

A QUICK POLL

Are you working remotely?

a. Yes, I usually or often work remotely
b. Yes, due to COVID
c. I was, but our offices are open again
d. No

Why work remotely?

Health concerns
- COVID-19
- Cold, flu, or other illness
- Doctor's appointment

Weather / Office Closure

Business travel

Personal time with a deadline you just can't miss

PRIVACY REF

Florida Government Finance Officers Association

Organizational Considerations

PRIVACY REF

Create a "work remotely" policy

Set clear expectations

Employee may be expected to:

- Choose a quiet and distraction-free working space
- Have an internet connection that's adequate for their job
- Dedicate their full attention to their job duties during working hours
- Adhere to break and attendance schedules agreed upon with their manager
- Ensure their schedules overlap with those of their team members (if necessary)
- Protect equipment
- Continue to comply with organizational policies

Organization may be expected to:

- Provide equipment
- Provide support services


Attendance
Social Media
Confidentiality
Privacy / Data Protection
Security
Bring Your Own Device
Employee Monitoring
Acceptable Use
Code of Conduct
Anti-discrimination
Dress code
Organizational Policies

PRIVACY REF

A QUICK POLL

Does your organization have a "working remotely" policy?

a. Yes
b. No
c. I am not sure

PRIVACY REF

Equipment – Bring Your Own Device

BYOD allows for you to use your personal devices for business

- Pros
- Cons

You must still adhere to Organizational Policies

- Confidentiality
- Privacy / Data Protection
- Security
- Appropriate Use
- Employee Monitoring
- Social Media

Organizations should consider a Mobile Device Manager

Tech Support concerns

PRIVACY REF

SECURING YOUR COMPUTER

Protect your data

- Lock your device
- Turn on device encryption
- Back up your data

Protect against threats

- Use anti-virus and anti-malware software
- Turn on automatic security updates, antivirus, and firewall

Beware of tech support scams

Know who else is using your computer

PROTECTING YOUR NETWORK CONNECTION

Connect to a safe network

- Use a wired, ethernet connection
- Use Wi-Fi encryption options for access

User Authentication

Virtual Private Networks

PRIVACY REF

User authentication

Username

- Identifies you
- Allows allocation of permissions

Password

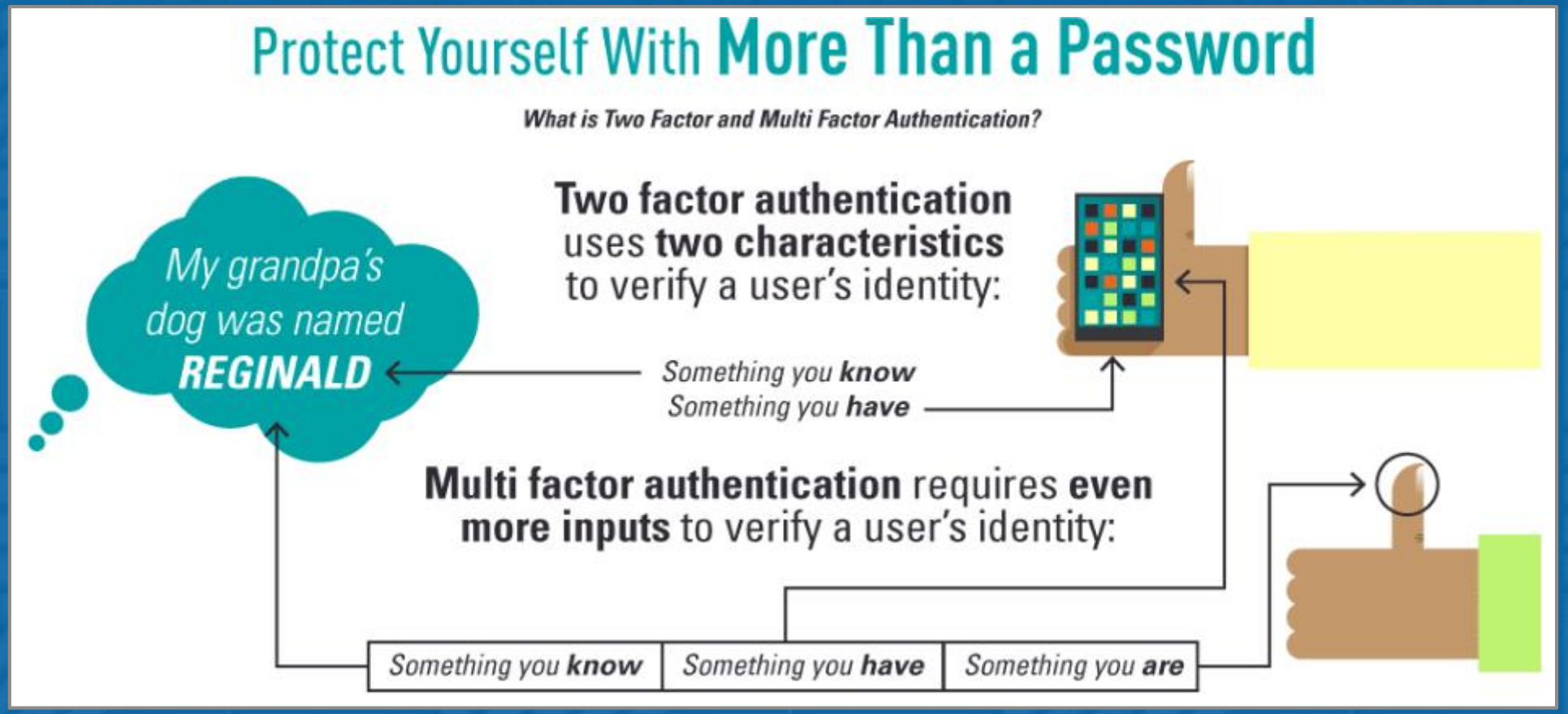
- A single factor of authentication
- It is something you know

Other factors of authentication

- Something you have
- Biometrics
- Where you are
- When you are

Provide a support line with authentication

MULTI-FACTOR AUTHENTICATION



PRIVACY REF

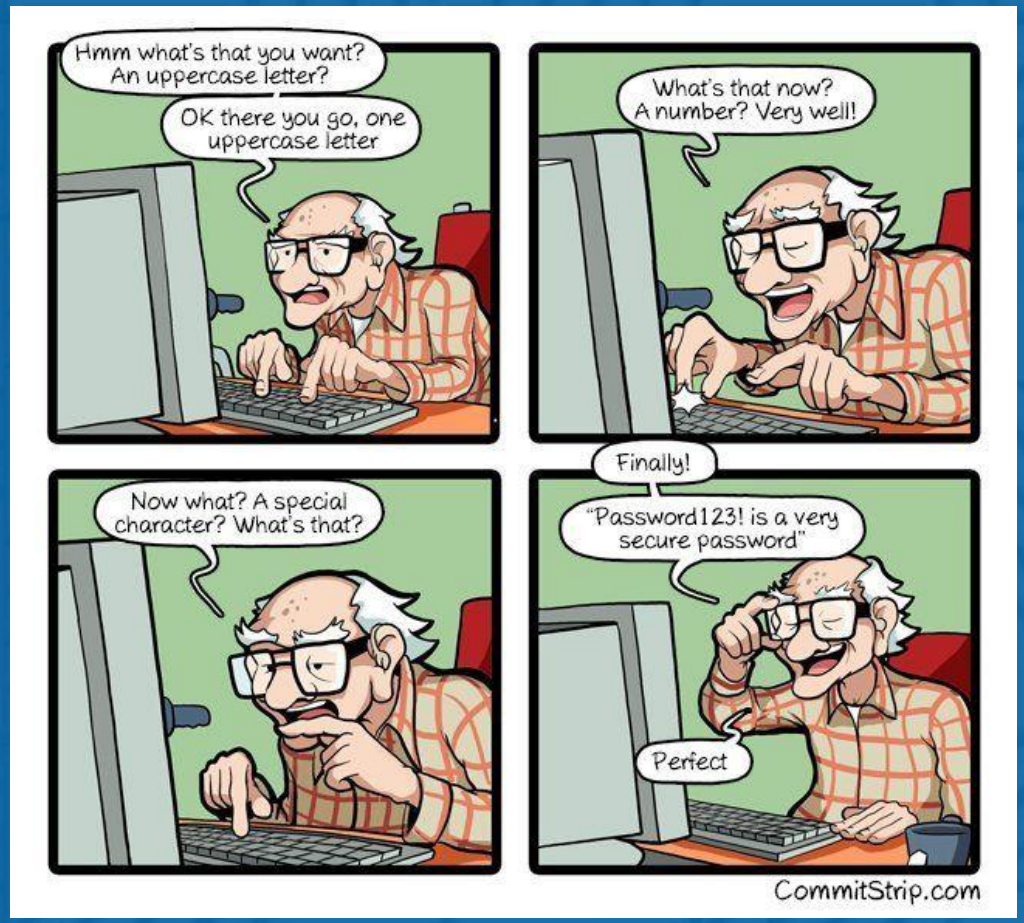
PASSWORDS

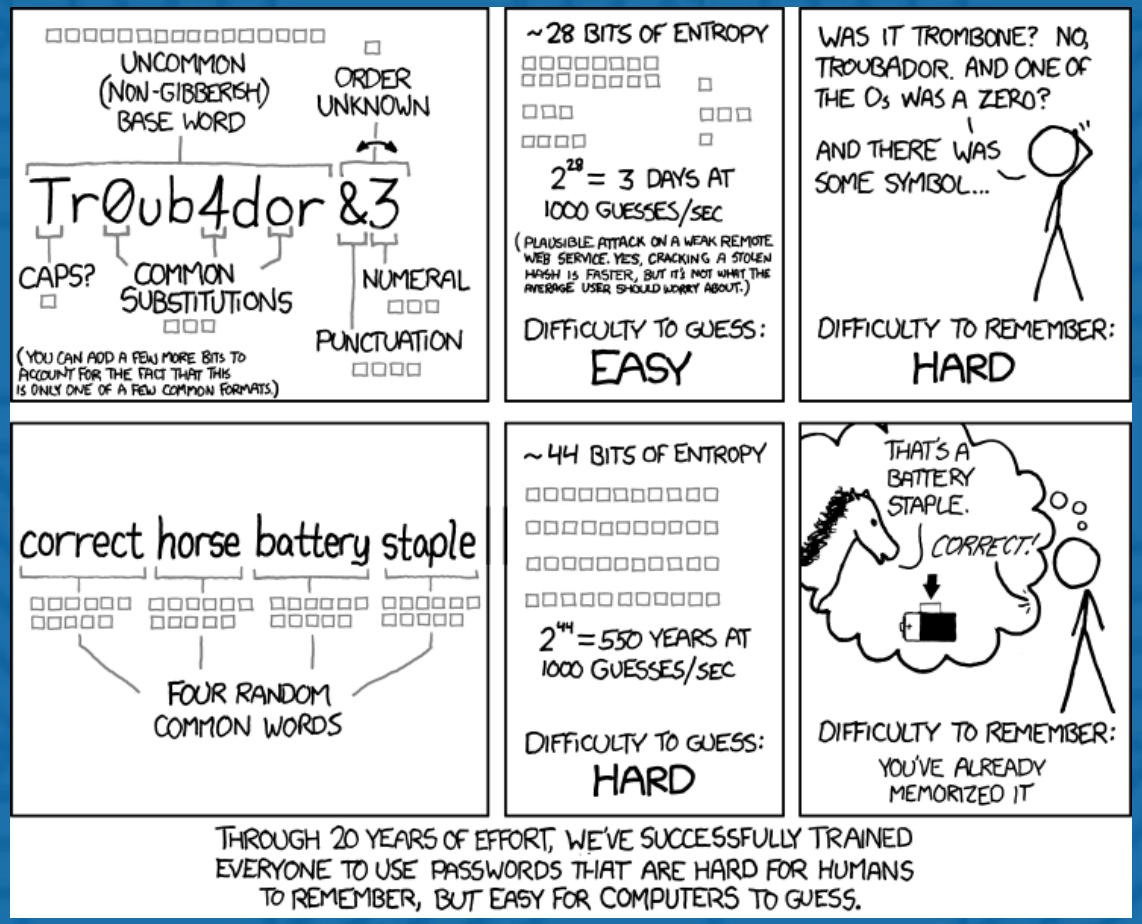
Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl

PRIVACY REF

ESTABLISHING STRONG PASSWORDS





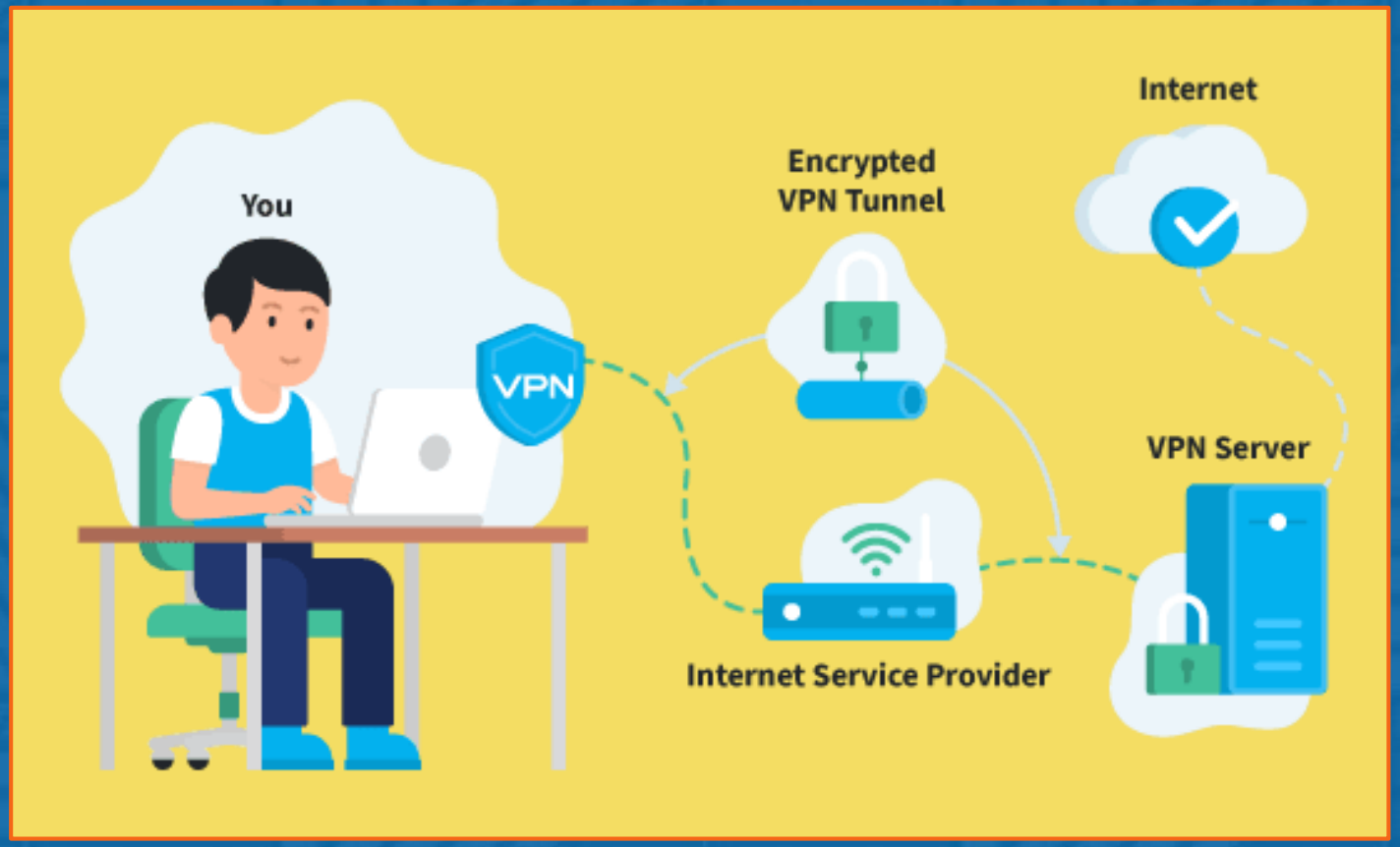
PRIVACY REF

Knowledge Check

Which of the following can be used to authenticate your identity?

a. Something you know
b. Something you have
c. Where you are
d. All of the above

Virtual Private Networks



PRIVACY REF

TIPS FOR USING YOUR MOBILE DEVICES

Mobile Device Management

Secure access to the device

- Password
- PIN
- Biometrics
- ~~Location~~
- ~~Connected devices~~

Know who you are sharing your device with

Be aware of your environment

- Beware of shoulder surfers
- On a phone keep your voice down
- Be cautious with backgrounds in pictures

PRIVACY REF

A REVEALING BACKGROUND

Handling confidential papers

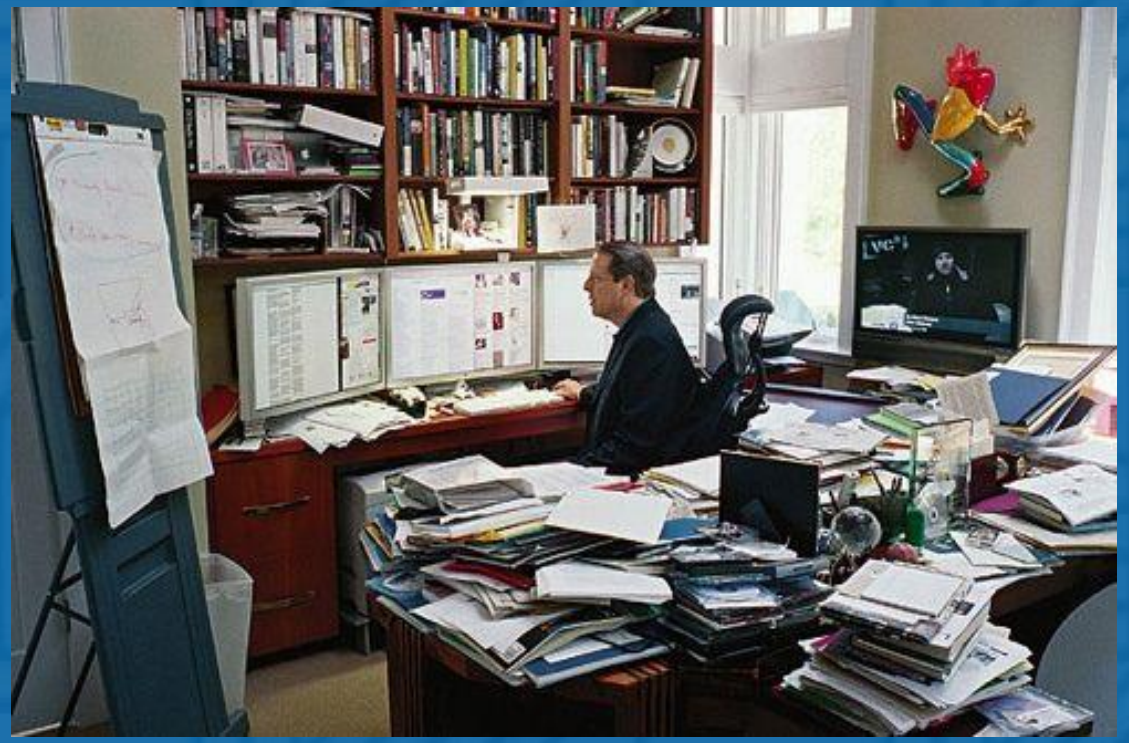
Follow your organizational policies

- Security
- Retention
- Destruction

Clean your desk

- Lock confidential material away
- Have a lock on the door

Have a shredder



PRIVACY REF

Knowledge Check

How should you destroy confidential papers?

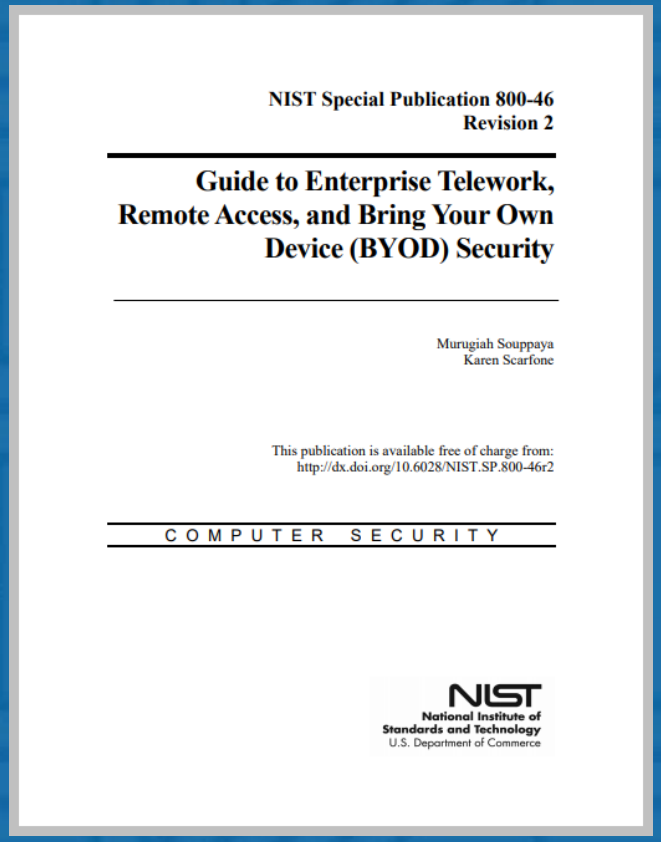
a. Throw it in the trash
b. Shred it
c. Use the back for notes

PRIVACY REF

NIST / Dept. of Commerce Guidance

NIST Special Publication 800-46 Rev. 2

Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security



NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-46r2

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PRIVACY REF

Florida Government Finance Officers Association

PERSONAL CONSIDERATIONS

PRIVACY REF

SETTING UP A HOME WORKSPACE

Quiet, distraction free

Proper equipment

- Computer
- Phone
- Shredder
- Locking cabinet or locked room

Monitors should not be viewed from the outside

Knowledge Check

Which is the better working arrangement?

a. Working in the bedroom

b. A dedicated space

PRIVACY REF

GUARDING AGAINST SCAMS

Social engineering

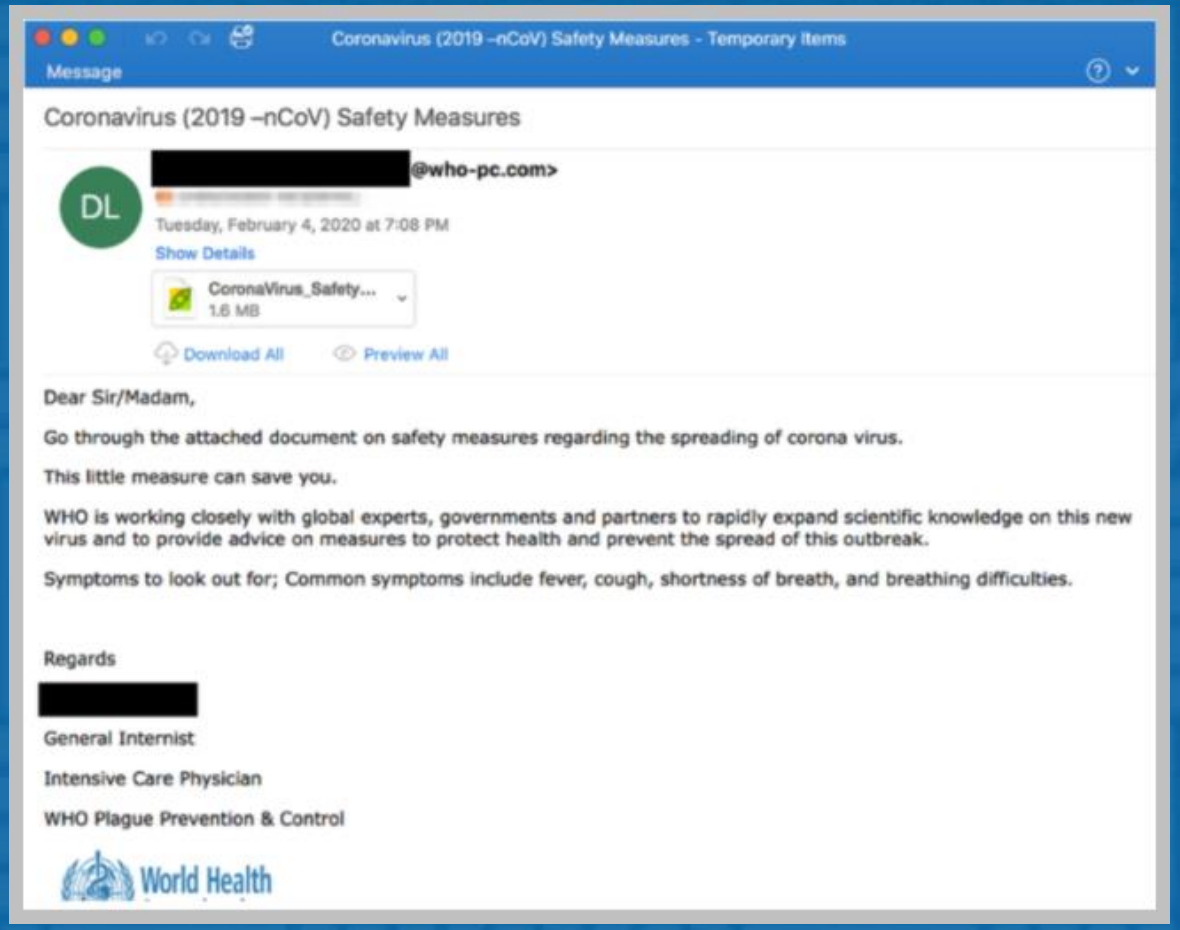
Phishing

Tactics

- Authority
- Urgency
- Emotion
- Scarcity
- Current events

PRIVACY REF

PHISHING EXAMPLES



Coronavirus (2019 -nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety...
1.6 MB

Download All Preview All

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[redacted]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control

World Health

---- Forwarded message ----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

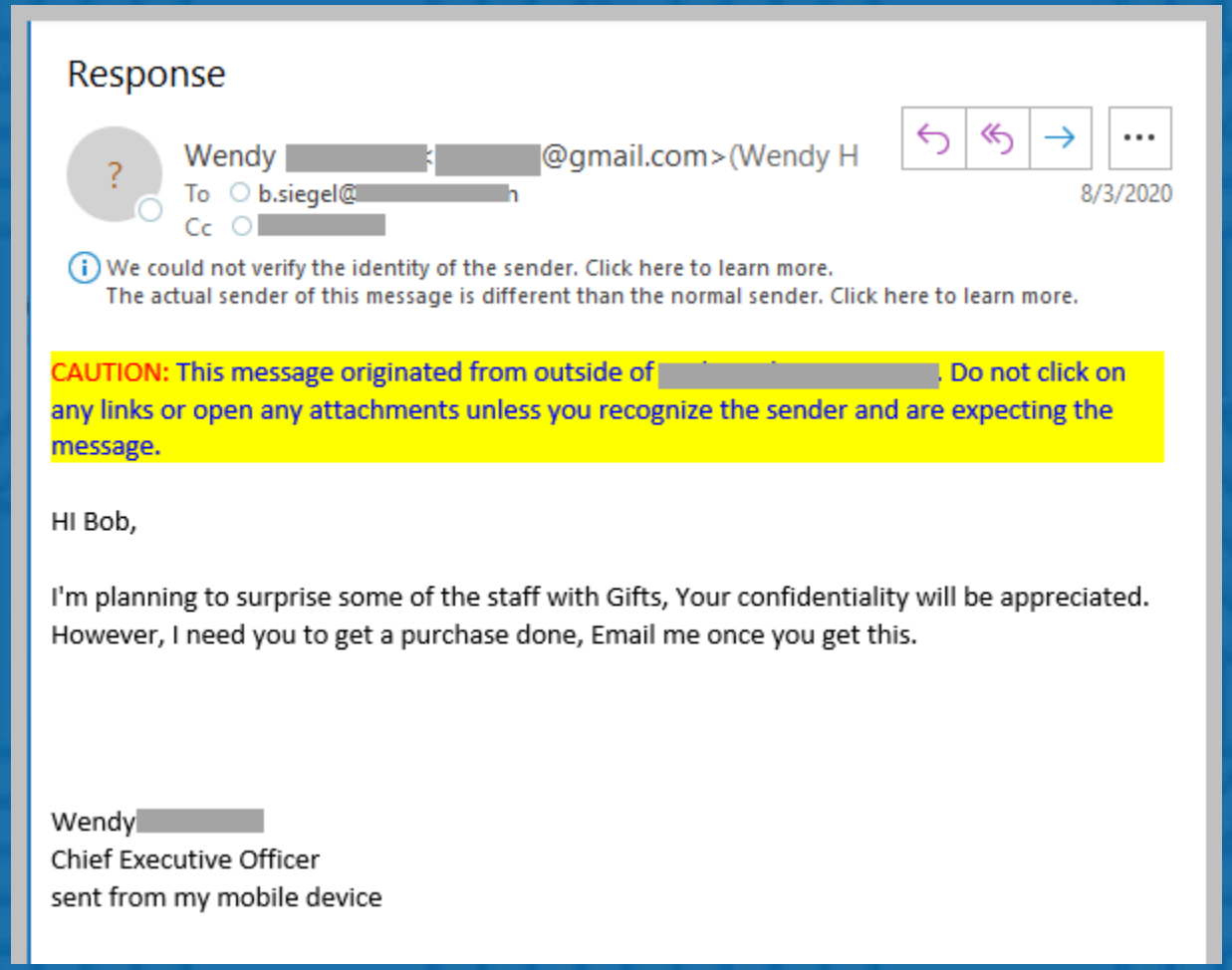
The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

PHISHING EXAMPLE



Response

Wendy [redacted]@gmail.com>(Wendy H

To b.siegel@[redacted]n

Cc [redacted]

8/3/2020

We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

CAUTION: This message originated from outside of [redacted]. Do not click on any links or open any attachments unless you recognize the sender and are expecting the message.

HI Bob,

I'm planning to surprise some of the staff with Gifts, Your confidentiality will be appreciated. However, I need you to get a purchase done, Email me once you get this.

Wendy[redacted]
Chief Executive Officer
sent from my mobile device

Knowledge Check

If you suspect an email is part of a phishing scam, you should…

a. Forward it to your friends
b. Open the attachments
c. Delete it
d. Send it to your boss

PROTECTING YOUR PERSONAL INFORMATION

Make sure people know you are in a meeting

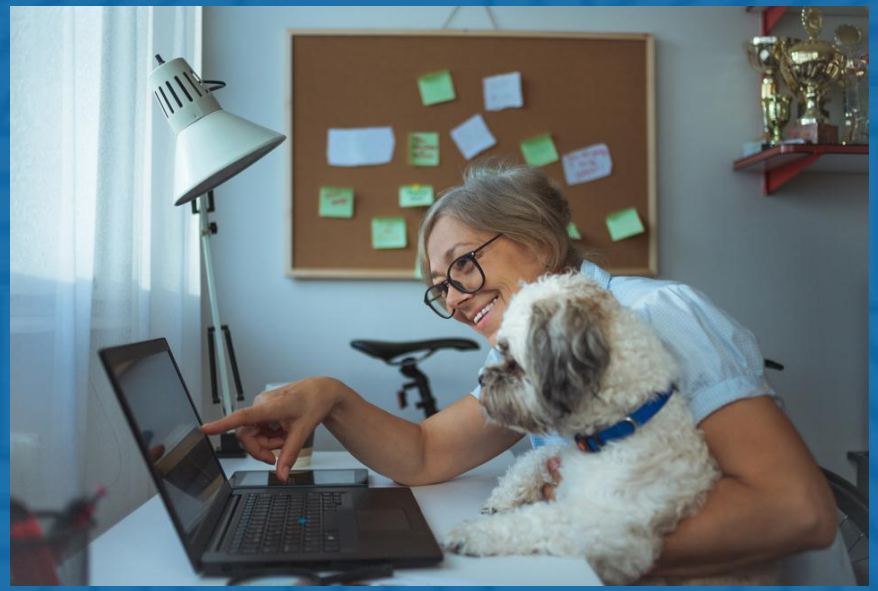
- Background conversations
- Drop ins by family and friends
- Visiting pets

Screen sharing

Video meeting background

PRIVACY REF

Good or Bad?

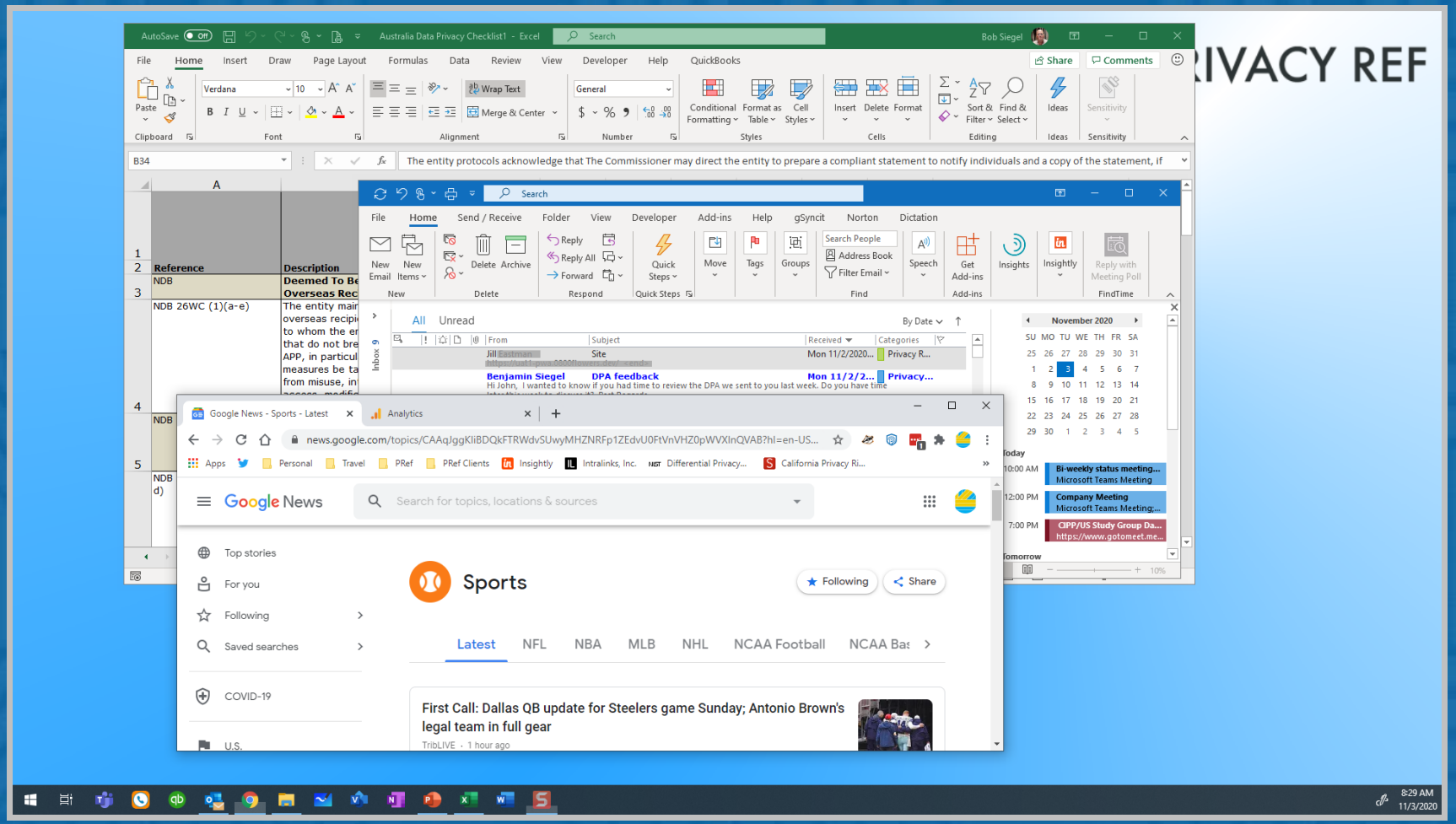


PRIVACY REF

Good or Bad Background?

PRIVACY REF

SCREEN SHARING



PRIVACY REF

Knowledge Check

Before sharing y
screen, you sho

hare

ot needed for

=YddwkMJG1Jo

PRIVACY REF

Best Practices for Remote Working

Organizational Considerations

1. Create a “work remotely” policy
2. Secure computers
3. Protect network connections
4. Establish strong passwords
5. Utilize a VPN
6. Properly use mobile devices
7. Protect confidential papers

Personal Considerations

1. Set up a home workspace
2. Guard against scams
3. Protect your personal information

THANK YOU

www.PrivacyRef.com

info@privacyref.com

@PrivacyRef

888.470.1528

PRIVACY REF