Leveraging Technology In Finance

Opportunity, Security and Contingency

#FLSOGF2022

PRESENTERS

Radcliffe Brown

Chief Operating Officer of Finance

Clerk of The Circuit Court & Comptroller, Palm Beach County

Parik Chokshi

Director

Clerk of The Circuit Court & Comptroller, Palm Beach County

Agenda

- Palm Beach County's Story
- Identifying and implementing opportunities to leverage technology
- System Contingency
- Fraud and need for system security
- Social Engineering
- Safe Computing
- Acceptable use Policy

Leveraging Technology In Finance - Current Objectives (PBC)

- Implement/Inject automation of business processes where feasible.
- Easier reporting and tracking of Key Performance Indicators (KPI).
- Flexibility.
  - KPI & Forecasting
  - Proactive vs Reactive
- Transparency.
- Minimize repetitive nonvalue added tasks using automation and AI where feasible.
- Process mapping documentation of all Finance Functions.

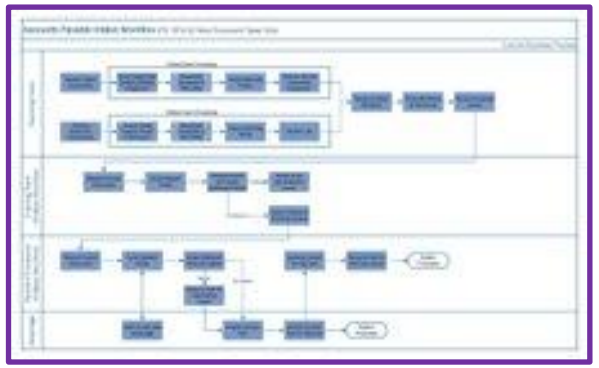
Leveraging Technology In Finance - Current Objectives

- Employees emphasis on problem solving and customer service.
- Increased productivity
- Reduced error rate.
- Improve customer satisfaction (Other Gov entities & public).

How Did We Get Here?

Scanning Project

Use of scanned images and digital information in existing business processes and reporting

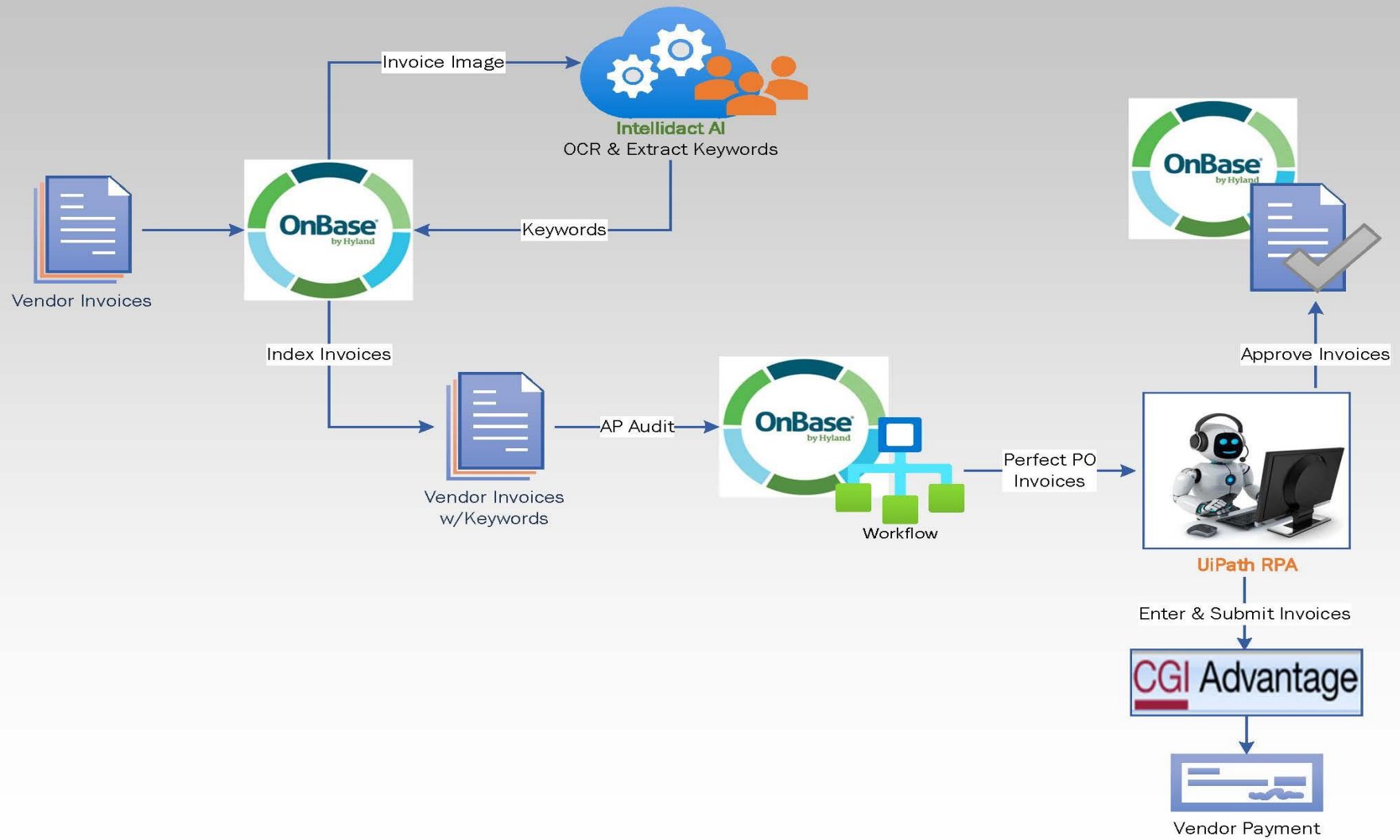


Implementation of modified business processes and workflows to take advantage of available digital technologies

How Did We Get Here?

Digitize Data & Documents	Manually Incorporated In Business Processes	Electronic Integration In Business Processes
Scanning Project: Receipt of information and data electronically	Use of scanned images and digital information in existing business processes and reporting	Implementation of modified business processes and workflows to take advantage of available digital technologies (OnBase Project)

OnBase Integration w/ AI & RPA and Advantage



Review & Understand Your Foundation

- People
- Infrastructure
- Data/information

Identify opportunities to leverage technology

- **Step 1. Establish/Understand Business Goals**
  - ✓What is our current objective to support the organizations long-term goals and objectives?
  - ✓Will automation help? If so, how and where?
  - ✓How will we monitor the success of the use of the technology?

Identify opportunities to leverage technology

- **Step 2. Identify Repetitive Tasks to Automate**
  - ✓ Use of graphical and visual representation of business functions.
    - ➢ Process Discovery Worksheet
    - ➢ Represented on Process Map/Workflow Diagram.
    - ➢ Helps identify inefficiencies and optimization opportunities.
  - ✓ Analyze and build on current workflows to enhance repetitive task-based workflows.
  - ✓ Identify and discuss with stakeholders.
  - ✓ Talk to your peers in and outside the organization.

Implement technology opportunities

- **Step 3. Choose/Plan the Suitable Workflow Automation & Vendor**
  - ✓Work with your IT or PMO team to define the scope of your project
  - ✓Communicate with a vendor that specializes in automation software and/or your ERP vendor.
  - ✓Type of Automation.
    - ➢Workflow
    - ➢Artificial Intelligence
    - ➢Robots/Bots (Attended & Unattended)

Implement technology opportunities

- **Step 3 (Contd.). Choose/Plan the Suitable Workflow Automation & Vendor**
  - ✓Proof of concept.
  - ✓Secure Funding if required.
  - ✓Create plan.

Implement technology opportunities

- **Step 4. Prepare the Management team and Workforce (change management).**
  - ✓Governance Board
  - ✓Obtain management approval and buy in.
  - ✓Involve impacted parties.
  - ✓Communicate.
  - ✓Training.
  - ✓Testing.

Implement technology opportunities

- **Step 5. Monitor and Track the Performance**
  - ✓ Track our goals
  - ✓ Recognize bottlenecks
  - ✓ Help decide areas for process improvement

System Contingency

- Work with your IT team and/or vendor to have a plan if the system in unavailable due to a disaster.
  - What are the critical processes that need to be up and how quickly
  - Communication (Who what when how)
  - Server Fire Example

Fraud and need for system security

- 2 Key Risk Factors relating to fraud in a digital environment
  - ➢Business Email Compromise (BEC)
    - Fraudsters impersonate vendor(s), executives or trusted partner.
    - AP, Procurement and Treasury targeted most.
  - ➢Online Account Take Over (ATO)
    - Gain access to make unauthorized transactions by stealing credentials of employees.
    - Gain access to a trusted device (laptop or workstation).
    - Misrepresent your organization to your business partners.

Fraud and need for system security

- Accessing and/or stealing your data (store only what is needed and encrypt what is held).
- Combating Business Email Compromise and Online Account Takeover requires security awareness.

Clerk of the Circuit Court & Comptroller

Security Awareness

Keeping You and the Organization Safe

#SOGF2024

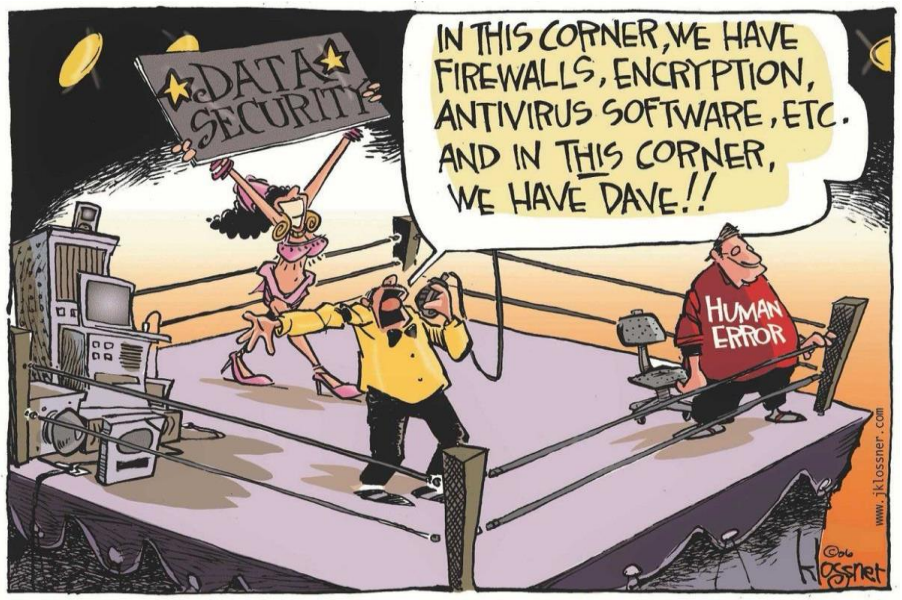
What are estimated cybercrime damages costs per year globally?

The Security Goal

Provide all stakeholders with a safe and secure technology environment and protect you from becoming a victim.

The BIG Misconception

"Security is an IT thing"

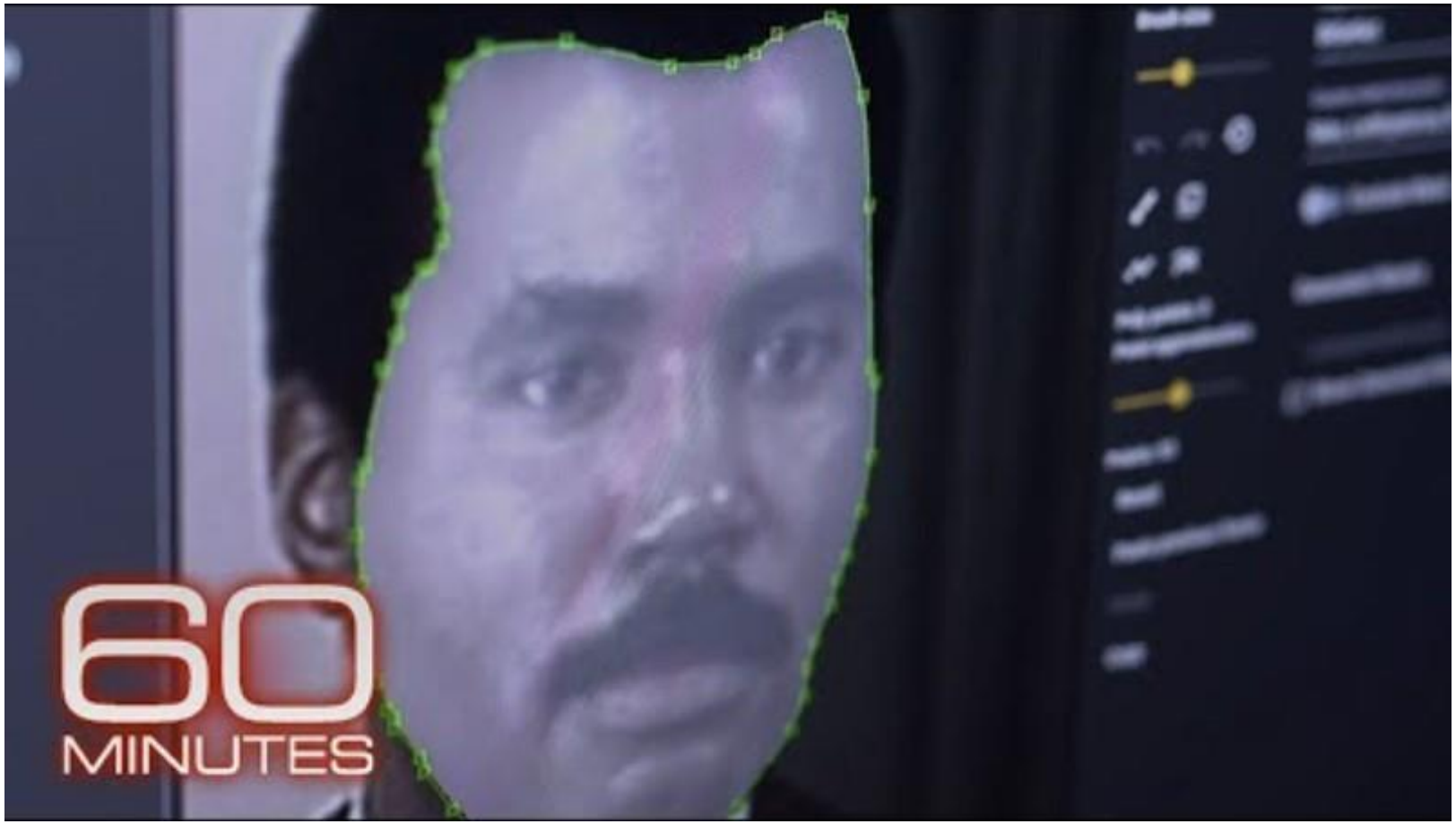


- Over 90% of breaches are due to human error
- Security is everyone's responsibility
- YOU are the first line of defense!!

Social Engineering

The clever manipulation of the natural human tendency to trust

New wave of social engineering fraud using AI

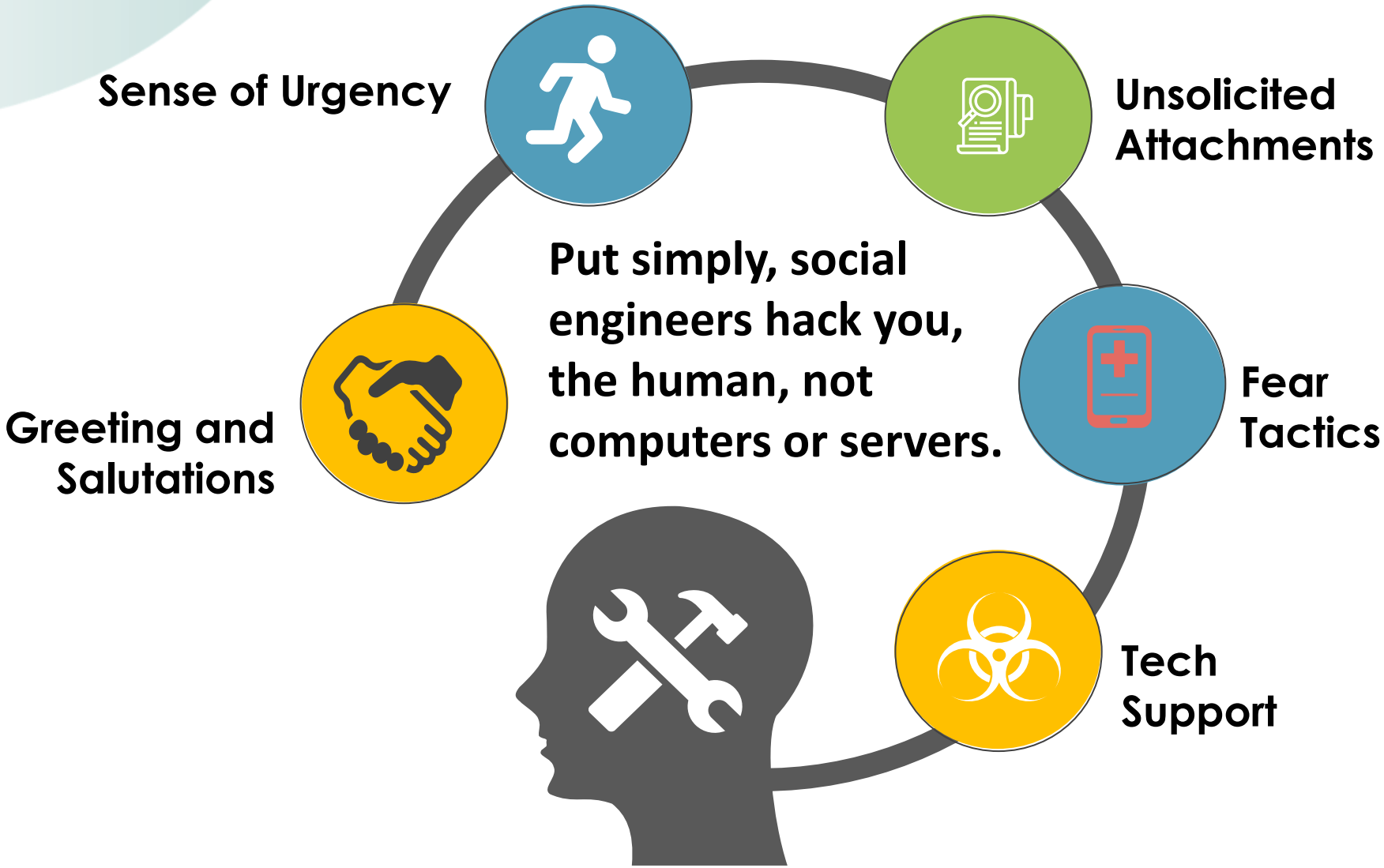


Social Engineering - Phishing

#1 Attack Technique

- Easy crime to commit
- Law of numbers
- Hard to track
- Lack of awareness

Social Engineering - *Red Flags*



Social Engineering - Phishing

- Pause and think before clicking on links or attachments
- Inspect the email
- Verify, verify, verify
- Be careful on your phone
- Never give out personal information
- Be on the lookout for scams
- If you do click, report it immediately

Phishing Example - Netflix

Vishing – Phone Scams

They sounded so legitimate

"Hello John, this is Bill from IT and I am updating your computer right now – but I need your password to install these new much-improved applications for you. You are going to love these new features!!!"

IT or any other legitimate organization will NEVER ask for your password or personal information.

Social Engineering - Physical Security

Circumventing Locks

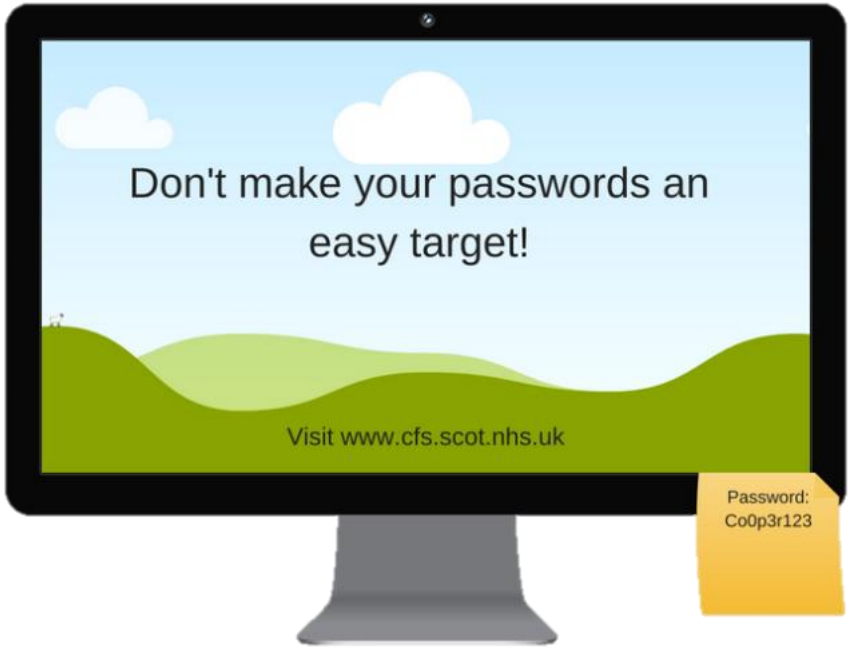
Piggybacking
(With Consent)

Tailgating
(Without Consent)

Safe Computing - Passwords

What makes you an easy target?

- Reusing passwords
- Writing passwords down
- Sharing passwords



Safe Computing - Passwords

- Use uppercase and lowercase letters
- Use symbols
- Use longer passwords
  - 8+ characters is OK, 12+ characters is better
- Use passphrases instead of single words
  - I.e., “Iam@SteelersFan4Life” vs. “Steelers”

Safe Computing – Multifactor Authentication (MFA)

What is MFA?

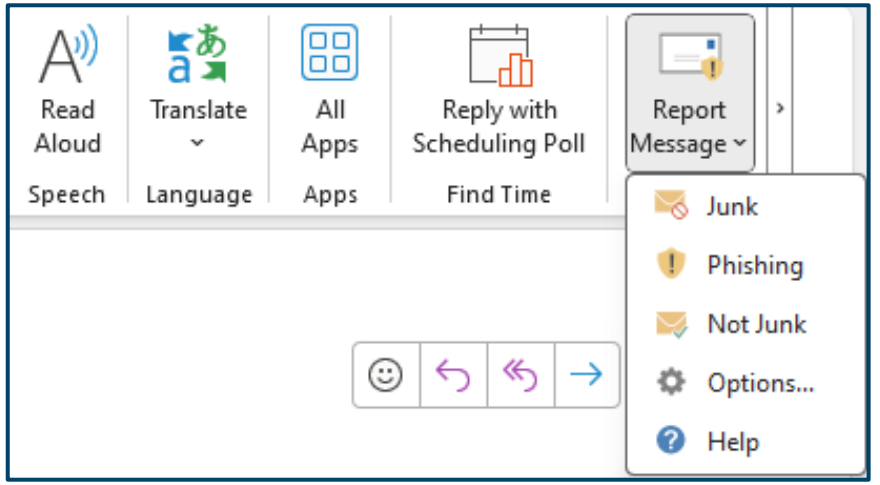
- MFA is authentication that must consist of at least two items:
  - Something you know, like a password
  - Something you have, like an authentication application
  - Something you are, like your fingerprint

- MFA can help block up to 99% of account compromise attacks

- Microsoft Authenticator mobile app is used for Clerk account authentication

Reporting Incidents - Time Is Of The Essence

- Report Phishing emails using the Report Message button
  - Only report emails that need further analysis by the IT Cybersecurity Team
  - If you do not need the IT Cybersecurity team's assistance with an email, you can just delete the email or mark it as Junk
- Report suspicious activity to the IT Service Center



Acceptable Use Policy

Administrative policy defining the dos and don’ts
for using Clerk information and equipment

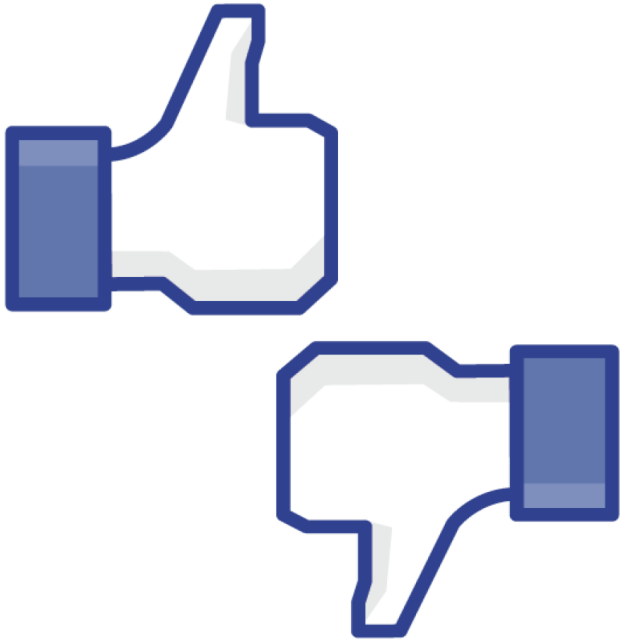
Business purposes - All Clerk systems are to be used for business purposes only

Other areas covered - Individual responsibility with respect to Privacy, Security, and Unacceptable Use

- Ensures your safety
- Protects the Clerk’s office
- Protects the citizens we serve

Acceptable Use Policy - What You Need to Know

Is this a do or a don't?



- Using unauthorized software to better do my job
- Adding copyrighted material to my presentation
- Reading work email
- Reading personal email on work equipment
- Running my own business on the laptop issued to me for remote work

Acceptable Use - What You Need to Know

Is this a do or a don't?

- Giving my password out to my supervisor in case I'm out of the office
- Clicking on links in emails
- Viewing personal Facebook while on work equipment
- Using authorized software to better do my job

Thank You

Any Questions?

#SOGF2024