Sec__ity;
U R at the Center

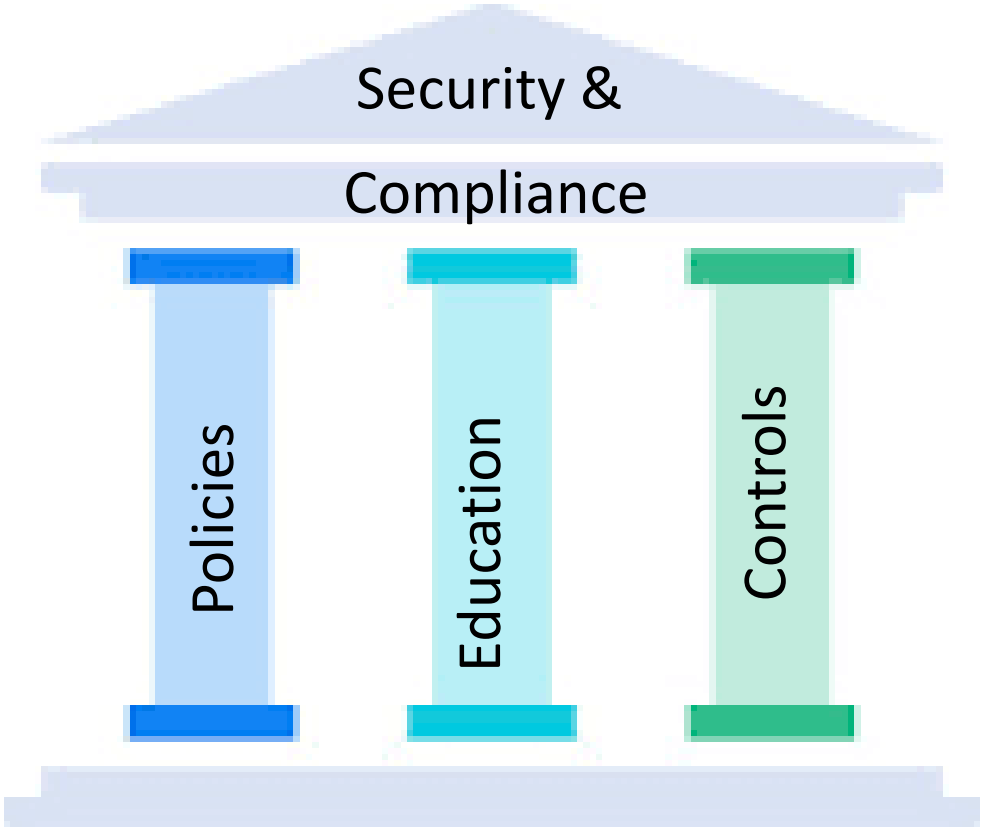
Gary Sheehan
Director – Information Security
April 2024

95% of cybersecurity breaches are attributed to human error – Allied World 2023

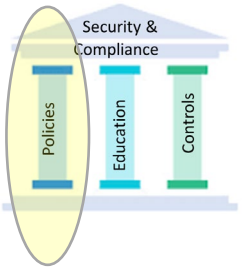
AGENDA:

- Elon’s Safety Zone
- Our Personal Safety Zone
- Hybrid Work Environment
- Need For Regulatory Compliance

Elon’s Safety Zone



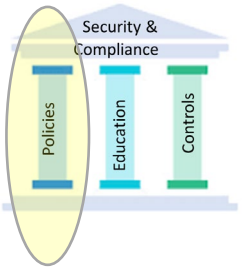
Elon's Safety Zone - Policies



- Policies
  - Information Security
  - Electronic Communications
  - Access Control
  - Acceptable Use
  - Account Management

All can Be Found on Elon's Information Technology Website

Elon's Safety Zone - Policies

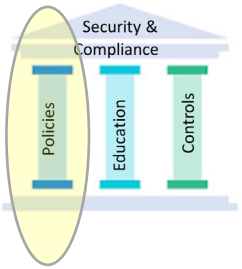


Important Policy Statements:

- Elon University will protect information and technology resources based on risk against accidental or unauthorized disclosure, modification, or destruction and ensure the confidentiality, integrity, and availability of Elon Data.

- Elon University will abide by all government and industry regulations related to information security, privacy and data protection.

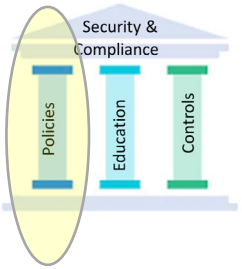
Elon's Safety Zone - Policies



Important Policy Statements:

- Each member of the Elon Community who accesses Elon's technology and Elon Data or assets is responsibility and accountable for all activity that is logged against their user-id.
- All employees that have Elon accounts are required to complete annual Information Security Awareness Training each academic year.
- Elon University owns the email system, network infrastructure and data, and reserves the right to examine any emails or files.

Elon's Safety Zone - Policies

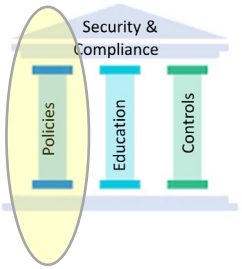


Important Policy Statements:

To protect the availability of the email services at Elon, Elon community members should refrain from the following activities:

- Excessive personal use
- Conducting unauthorized access of other people's email
- Sending 'SPAM', chain letters, letter bombs or any other type of widespread distribution of unsolicited email
- Giving the false impression you are representing the University
- Using an Elon email account for commercial or personal activities
- Sending of offensive or abusive messages
- Conducting unlawful activities

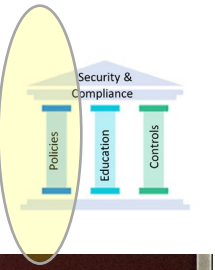
Elon's Safety Zone - Policies



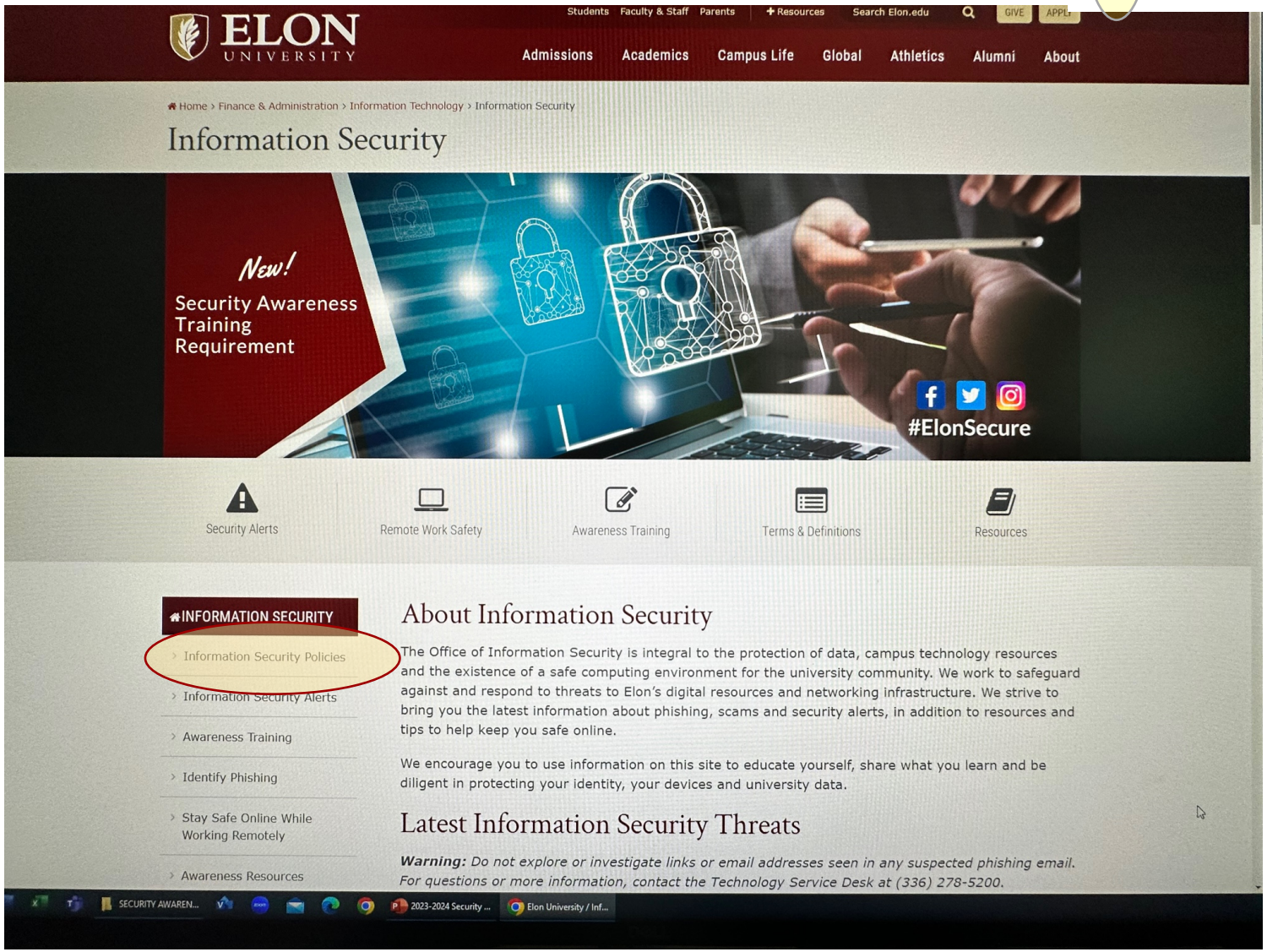
Important Policy Statements:

- Elon computer and network access accounts will be created and managed according to information security standards and business requirements.
- When faculty or staff members resign or are terminated, their accounts are disabled immediately after their last day of employment and deleted 60 days later.
- All Elon network accounts, regardless of affiliation will be disabled after 365 days of inactivity and deleted after 180 days in disabled status.

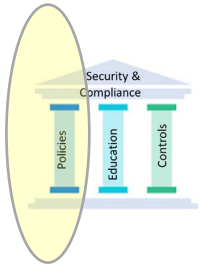
Elon's Safety Zone - Policies



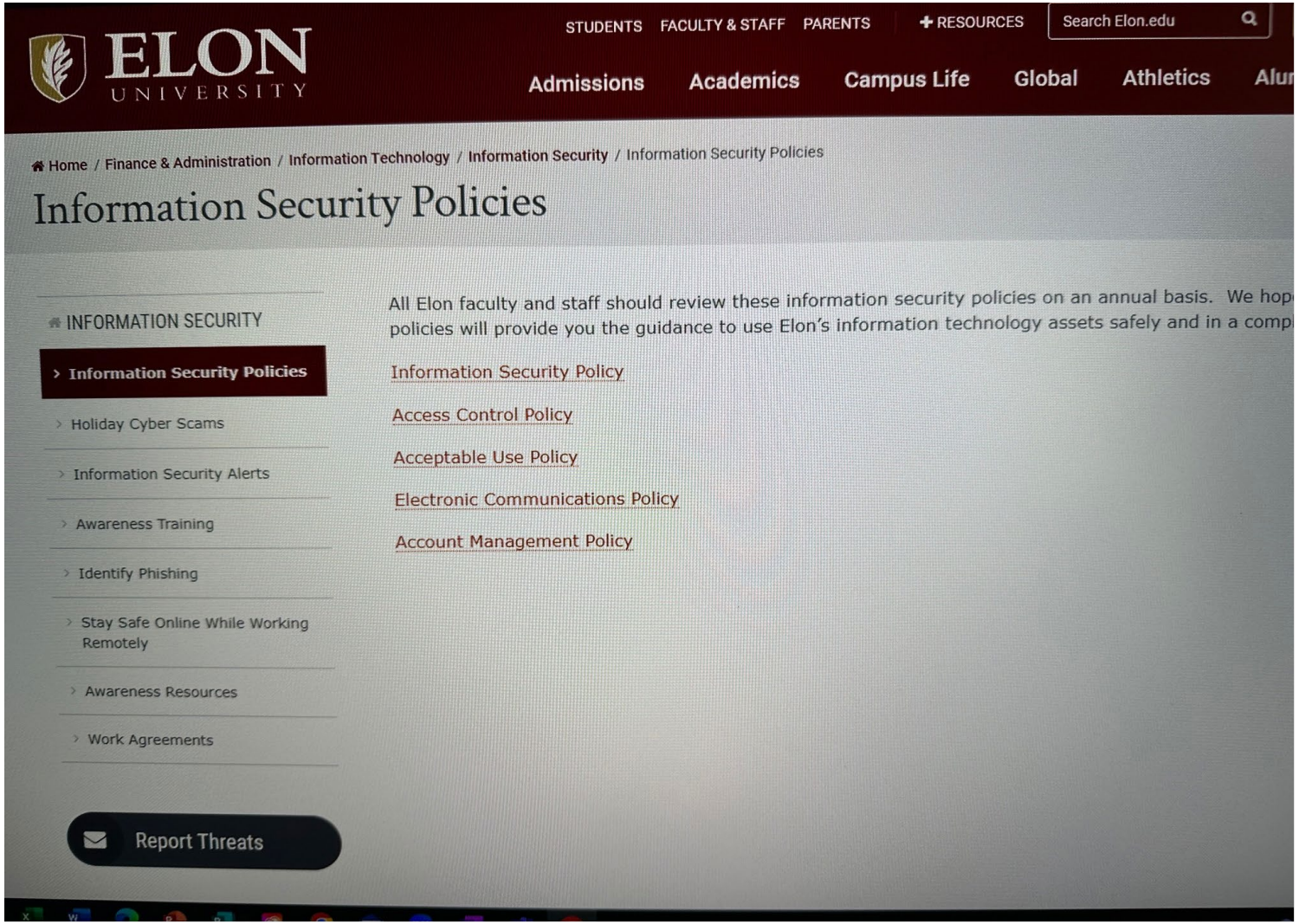
You can find all the policies related to Information Security on our website.



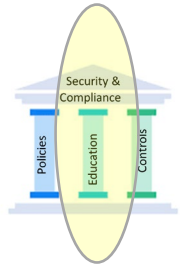
Elon's Safety Zone - Policies



You can find all the policies related to Information Security on our website.



Elon's Safety Zone– Education & Awareness

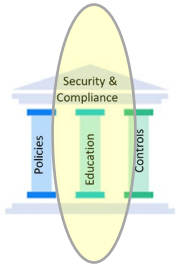


Stay Informed

Elon's Security Awareness Program includes:

- An Information Security Alert System
- A video library (Moodle)
- New employee orientation information
- Periodic training events throughout the year
- Easy ticket submission (*infosec@elon.edu*)
- Awareness resources available

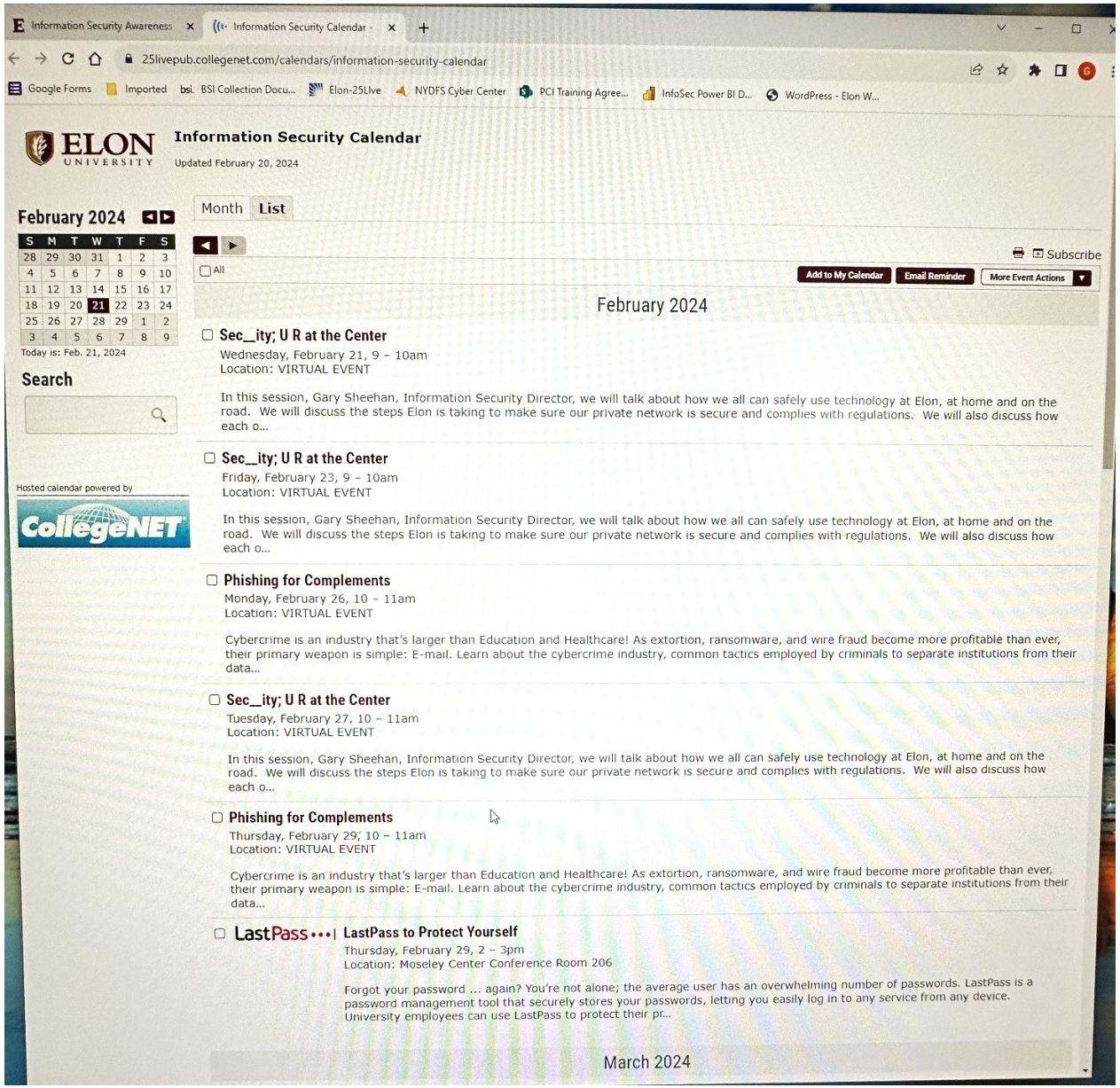
Elon's Safety Zone– Education & Awareness



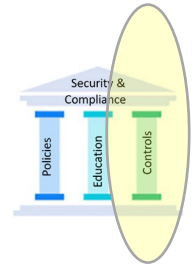
Stay Informed

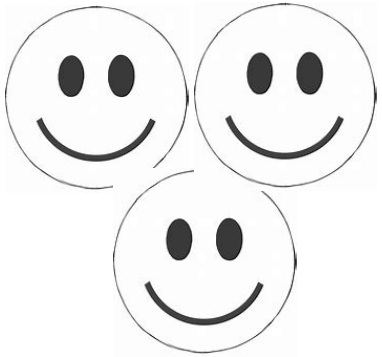
Elon's Security Awareness Program includes:

- An Information Security Alert System
- A video library (Moodle)
- New employee orientation information
- Periodic training events throughout the year
- Easy ticket submission (*infosec@elon.edu*)
- Awareness resources available



Elon's Safety Zone – Controls





Log Monitoring
Web Filtering
Application Restrictions
Compliance Controls

Data Loss Prevention

Data Loss Prevention

Multifactor authentication

DNS / IP / App Blocking

IDS / IPS

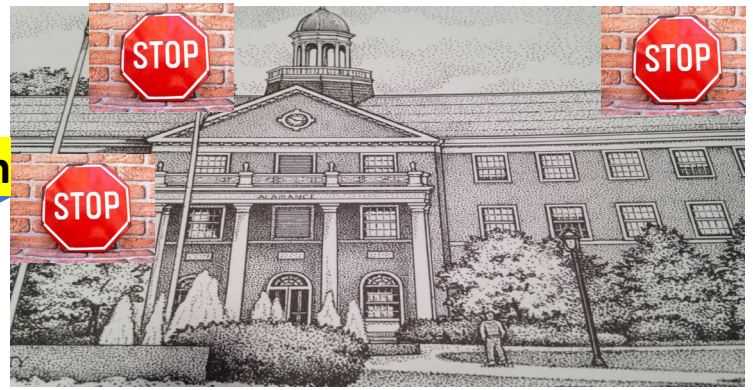
IDS / IPS

DNS / IP / App Blocking

Log Monitoring
Web Filtering
Vulnerability Scanning

Endpoint Controls
Software Updates
Data Encryption
Problem Management
Policies

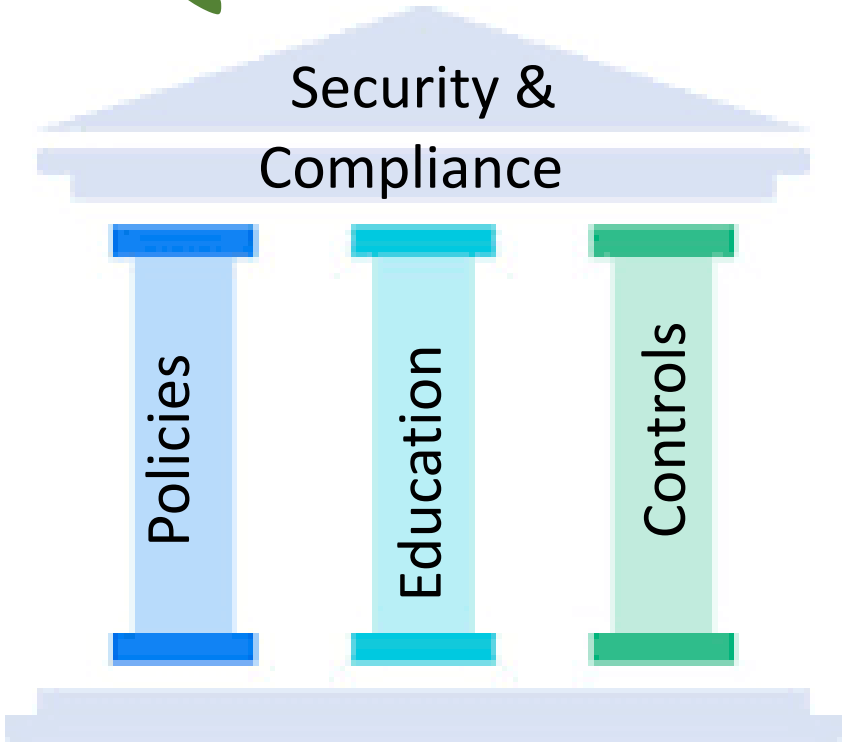
Multifactor authentication



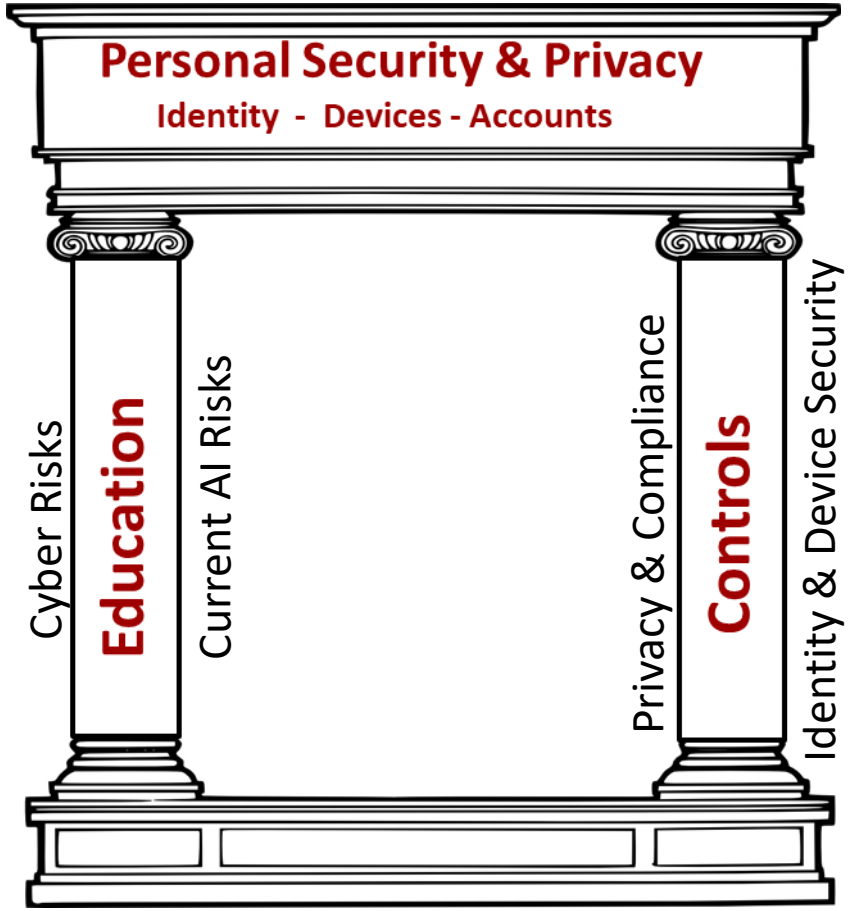
Security Awareness / Education

Elon’s Safety Zone

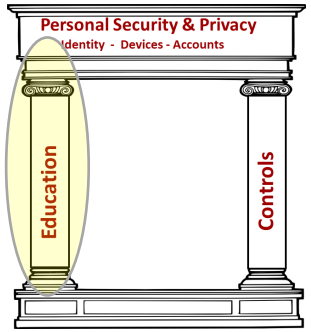
ANY QUESTIONS?



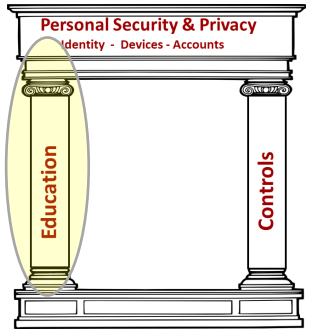
Our Personal Safety Zone

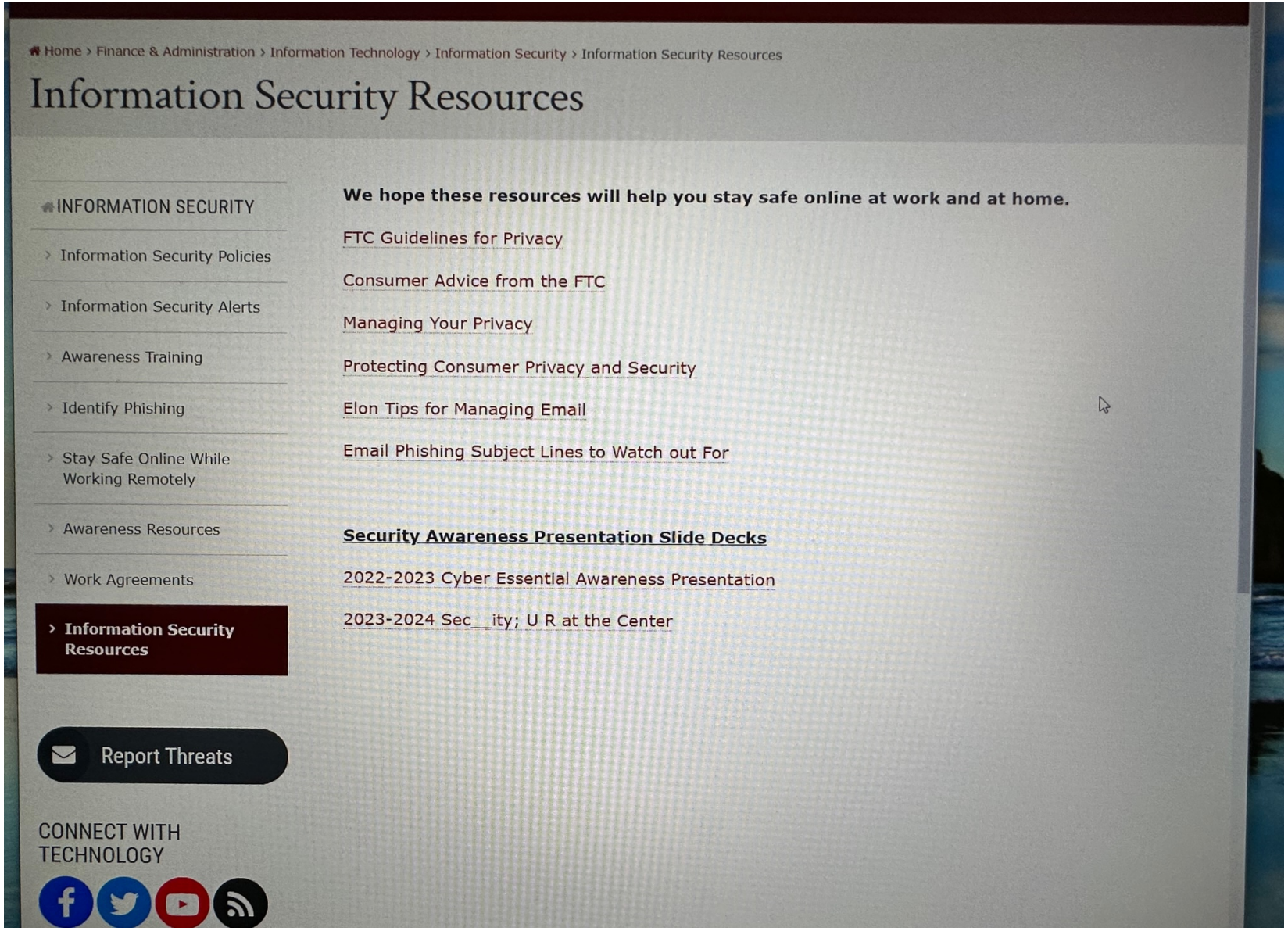


Our Personal Safety Zone - Education & Awareness

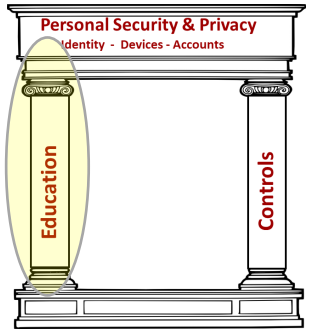


Our Personal Safety Zone – Education & Awareness





Our Personal Safety Zone – Education & Awareness



What is AI?

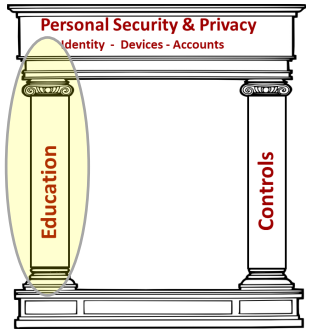
Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include expert systems, natural language processing, speech recognition and machine vision.

Current AI-related Risks?

1. Consumer privacy/security/compliance
2. Biased programming & results
3. Physical danger to humans
4. Destructive behavior / Deepfakes
5. Unclear legal regulation

Do the current benefits outweigh the risks?

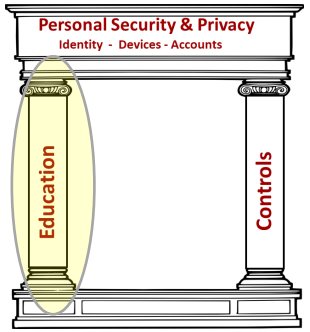
Our Personal Safety Zone – Education & Awareness



So – What Can We Do To Protect Ourselves Today?

- Don’t be afraid of AI
- Avoid putting/using confidential information into an AI platform
- Make sure to review and validate any output from an AI-generated response
- Clearly indicate when your content is AI-generated
- Before using AI for Elon purposes, make sure legal and compliance are onboard

Our Personal Safety Zone – Education & Awareness



- Data Back-ups
- Always run software updates – (auto update is best, OS & Apps)

- Enable strong user authentication – (Screen lock / Biometrics, etc.)
- Avoid public wi-fi – (increased exposure to malware and hackers)
- Secure your home network – Check with your ISP
- Practice good application security & privacy, beware of malicious apps
- Be cautious of phishing scams and spoofed email
- Use Social Media wisely

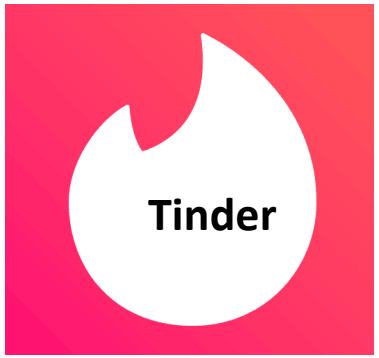
Our Personal Safety Zone – Education & Awareness

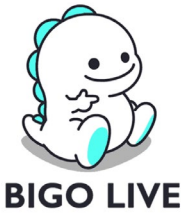
Social Media is the Biggest Risk to Privacy

- Be cautious about what you post in Social Media
- Be careful when accepting “Friend” connections
- Search yourself on Google – see what is public
- Consider posting your vacation photos & plans AFTER you get home
- Restrict who can see your friends list, contacts and photos
- Posting photos of job offers or college acceptance letters might reveal too much personal information

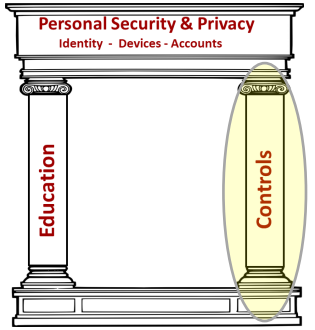
Our Personal Safety Zone – Education & Awareness

18 Most Dangerous Apps for Children in 2023





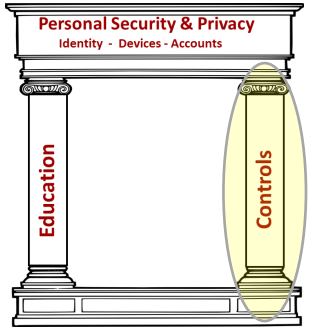
Our Personal Safety Zone – Controls: Device Security



Many of the advances in technology that make our lives easier and more comfortable, also are the biggest threats to our personal privacy.

Social Media
Trackers
Smart Devices
Voice Technology
AI
GPS
Facial Recognition
Camera Technology
Analytics

Our Personal Safety Zone – Controls: Device Security



Privacy Configuration Settings on Mobile Include:

- Location settings / GPS
- Tracking (tracking application use activity)
- Access to your camera
- Access to your microphone
- Access to contacts & calendars
- Fitness / Activity tracking
- Access to your photos
- Access to files and folders
- Bluetooth access
- Access to reminders

Our Personal Safety Zone – Controls: Device Security

Gary's General Rules:

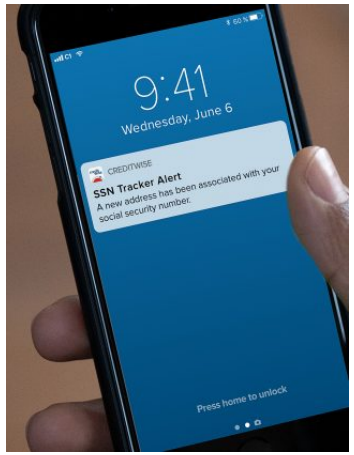
- Grant only required privileges for services
- Review location settings
  - always-on vs. in-use only
- Review Microphone/Camera settings
- Delete all unused apps from your phone.

Our Personal Safety Zone – Controls Privacy

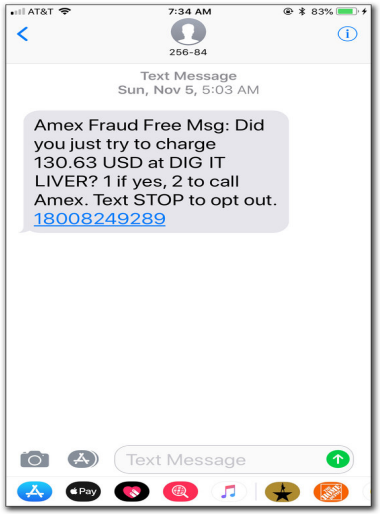
- Identity Protection Services
- Credit Card Purchase Protection
- Credit Card Fraud Protection
- Credit Monitoring

IdentityProtectionReview.com

Purchase alerts are useful for tracking charges made to an associated credit card.

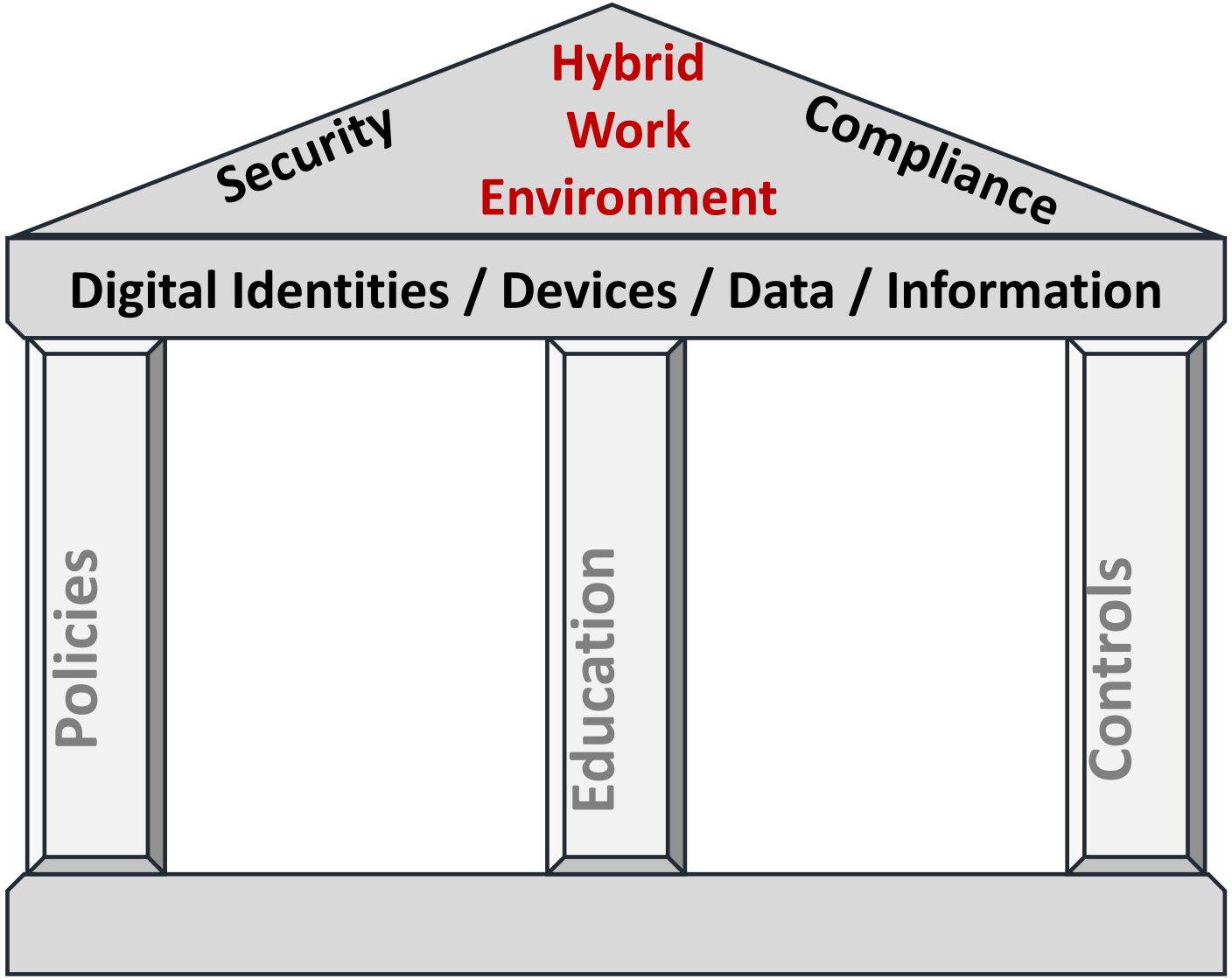


Fraud alerts are especially useful for stopping fraudulent charges in their tracks



THE HYBRID WORK ENVIRONMENT

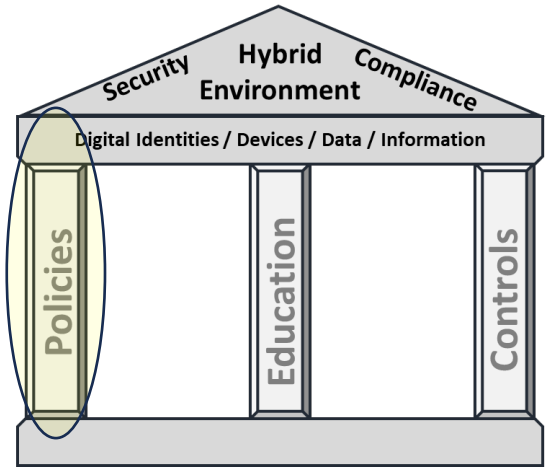
Keeping Safe in a Hybrid Work Environment



Keeping Safe in a Hybrid Work Environment - Policies

Policy Requirements:

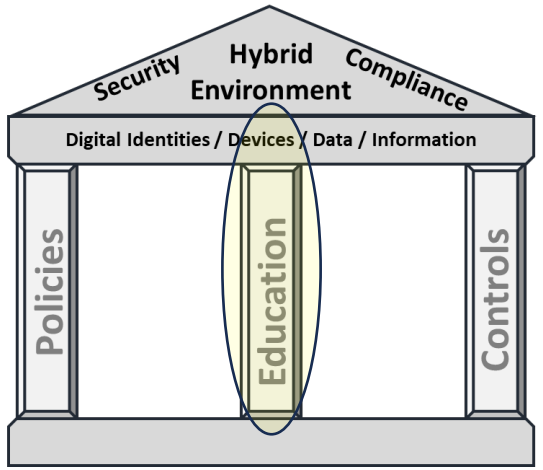
- Administrative & Technical
  - Policies should address the workplace expectations and responsibilities.
  - Policies should address technical requirements for supporting a telework/remote environment
  - All policies must support Boldly Elon



Keeping Safe in a Hybrid Work Environment - Education

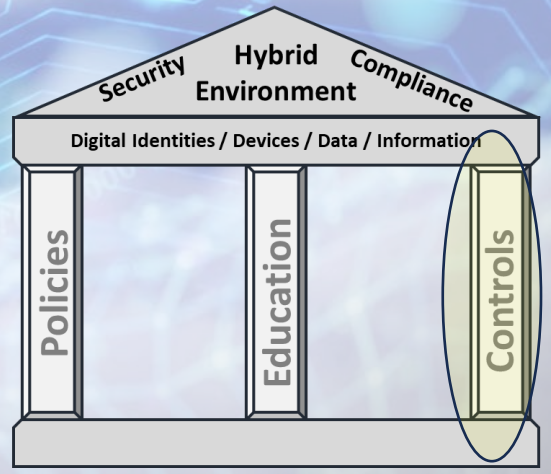
There is always free cheese in a mousetrap.

Don’t get caught in the trap.



Keeping Safe in a Hybrid Work Environment - Controls

- **Technology Controls in a Hybrid Work Environment**
  - Digital Identity Management
  - Device authentication
  - Device security
  - Strict password management



Keeping Safe in a Hybrid Work Environment - Controls

What is LastPass ?

- Only remember one password
- Easily retrieve passwords, on any device, through your LastPass vault
- Create secure passwords through the LastPass password generation tool
- Mobile app
- Easily and securely share passwords with work a team
- Can be shared with family members

Compliance is Key

Regulatory compliance requires a business follow state, federal, and international laws and regulations relevant to its operations.

Compliance is Key

Area of Compliance	Number of Requirements
Finance (Tax, Accounting, Donors, Financial Aid)	79
Academic	27
Campus Safety	7
Copyright	7
Disabilities Accommodations	13
Environmental	28
Export Controls	8
Health Care	3
Human Resources	54
IT / IT Security	34
Research	7
Miscellaneous	20
	287

Compliance is Key

Requirement	Data / Information Impacted	Responsibility
Title IV / - Financial Aid	Manages federal funds disbursed to a student's account in excess of allowable charges.	Patrick Murphy
Health Insurance Portability and Accountability Act **(HIPAA)**	Medical / health related information for all individuals.	Jana Lynn Paterson
Clery Act	A consumer protection law that aims to provide transparency around campus crime policy and statistics.	Sgt. Paul Smith
Title IX	Prohibits sex-based discrimination in any school or any other education program.	Megan Karbley
National Collegiate Athletic Association **(NCAA)**	Institutions must conduct their athletics programs with integrity and in compliance with conference and NCAA rules and regulations.	Jeffrey Scheible
The Americans with Disabilities Act **(ADA)**	Protects the civil rights of people with disabilities in many aspects of public life.	Megan Karbley
Payment Card Industry Standard **(PCI-DSS)**	Credit card processing formation – electronic commerce	Gary Sheehan
Unrelated Business Income Tax **(UBIT)**	Managing tax and tax data on unrelated business income	Susan Kirkland
General Data Protection **(GDPR)**	Personally Identifiable Information for European Union citizens	Gary Sheehan
Gramm-Leach-Bliley Act **(GLBA)**	Student financial information and other non-public student information	Susan Kirkland
Family Educational Rights and Privacy Act **(FERPA)**	Student non-public personal and academic information	Rodney Parks
State Privacy Laws (PII)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.	All Employees

Compliance is Key

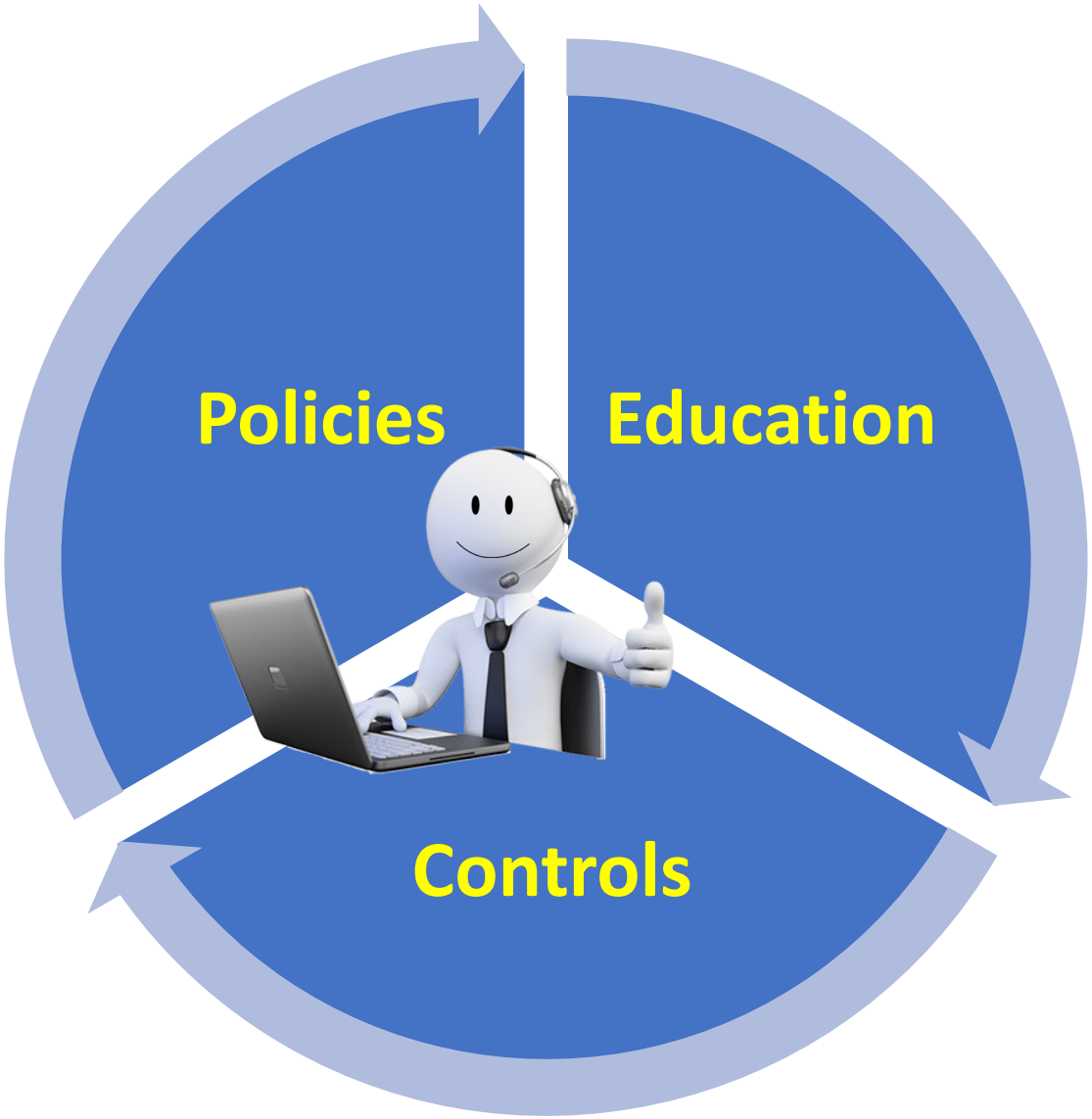
Everyone who handles, accesses, stores, transmits or processes regulated data or sensitive data has a responsibility to be aware of and comply with regulatory requirements.

Personal information, when misused or inadequately protected, can result in identity theft, financial fraud, regulatory non-compliance and other problems that collectively cost people, businesses and governments millions of dollars per year.

Summary

- Working at Elon
- Teleworking
- Hybrid Environment
- Compliance

  - Policies
  - Education
  - Controls



We all must do our part to Ensure Cyber Safety, Data Privacy & Compliance

Q & A

Feedback is welcome and appreciated.