Sec__ity;
U R at the Center

Gary Sheehan
Director – Information Security
June 2023

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

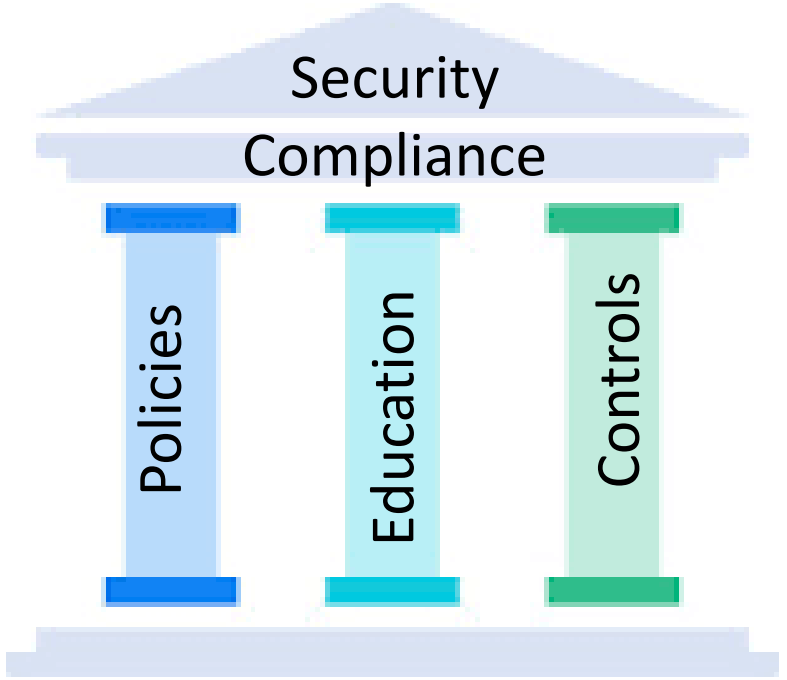
AGENDA:

- Working Safe at Elon
- Keeping Yourself Safe
- Hybrid Work Environment

Keeping Safe at Elon

To keep our Elon community safe, we focus our efforts on 3 Safety Pillars:

- Policies
- Education & Awareness
- Controls



Keeping Safe at Elon - Policies

Policy Requirements:

- Policies
  - Information Security
  - Electronic Communications
  - Access Control
  - Acceptable Use
  - Account Management (*coming soon*)

All can Be Found on Elon's Information Technology Website

Keeping Safe at Elon - 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.

Keeping Safe at Elon - 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 his or her user-id.

- All employees that have Elon accounts are required to complete annual Information Security Awareness Training each academic year.

Keeping Safe at Elon - Policies

Important Policy Statements:

- Elon University owns the email system, network infrastructure and data, and reserves the right to examine any emails or files.
- Elon University's access control mechanisms are designed to minimize risk and potential exposure to the University resulting from unauthorized or malicious use of resources.
- Elon University will apply appropriate internal controls implementing "least privilege" and "need to know" principles guided by Elon's "Access Control Policy" and "Acceptable Use Policy."

Keeping Safe at Elon - Policies

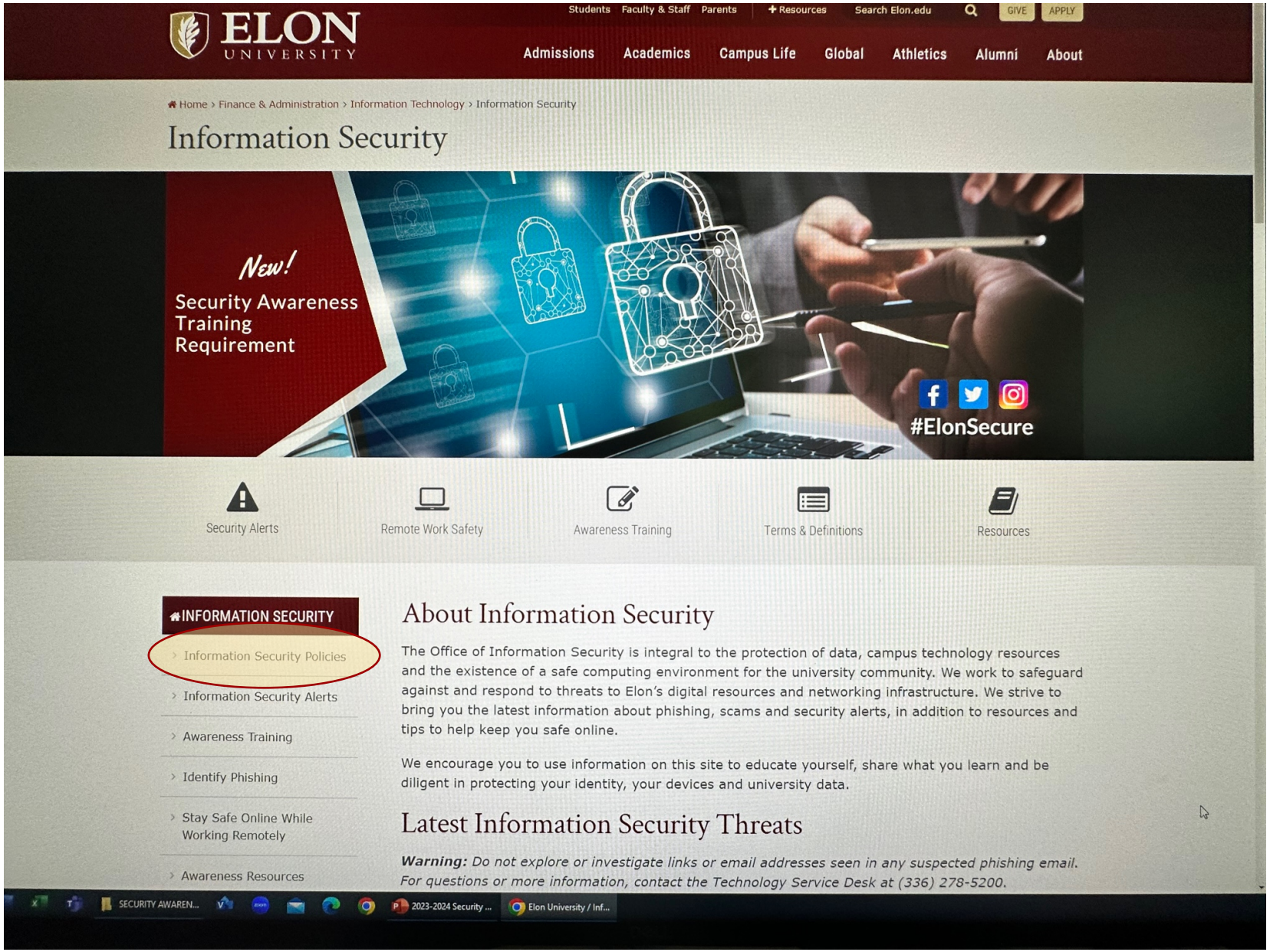
Important Policy Statements:

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

- Excessive personal use
- Intentional unauthorized access of other people's email
- Sending 'spams', chain letters, letter bombs or any other type of widespread distribution of unsolicited email
- Forging/Spoofing 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
- Spoofing, forging, altering, or removing of electronic mail headers

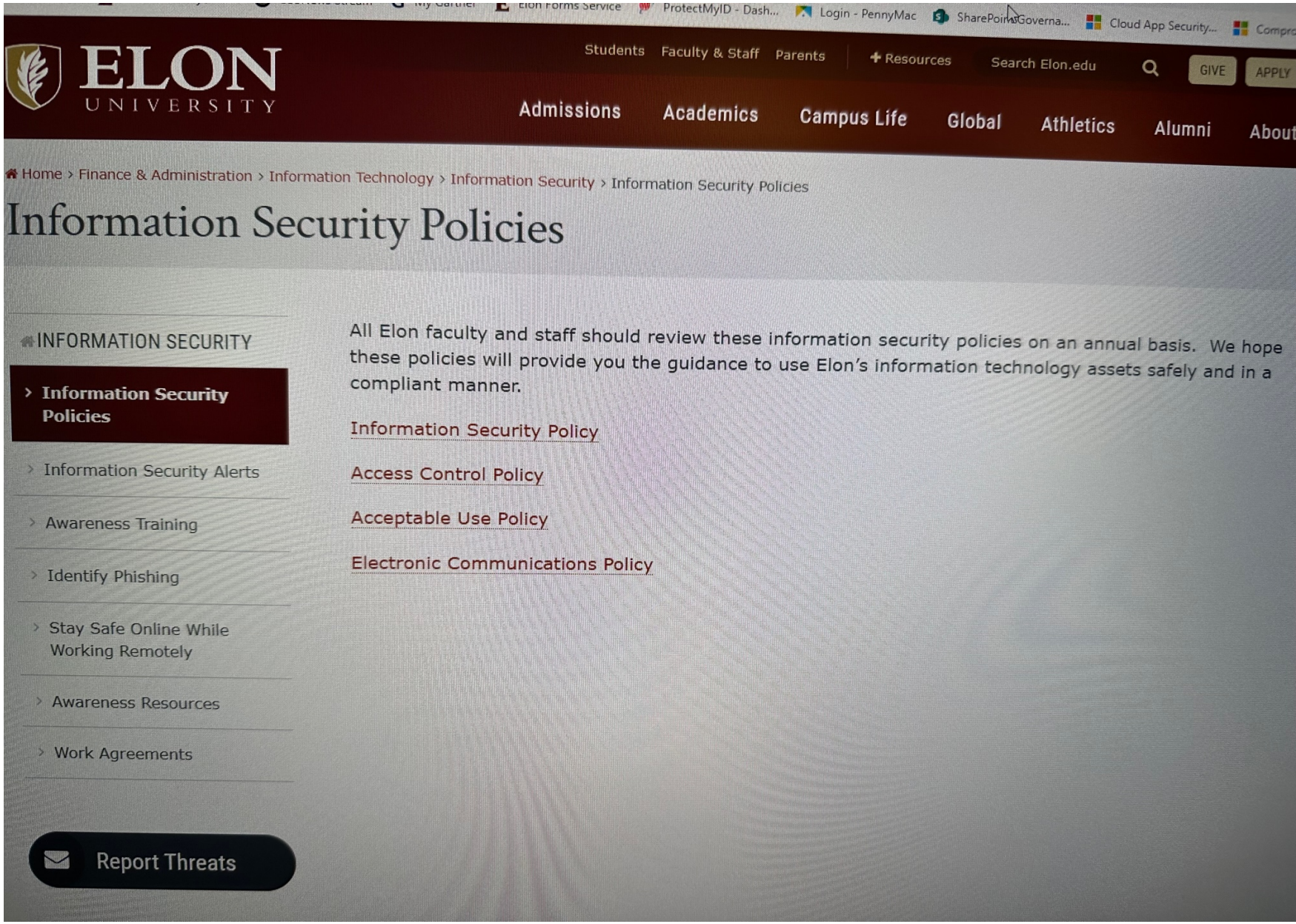
Keeping Safe at Elon - Policies

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



Keeping Safe at Elon - Policies

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

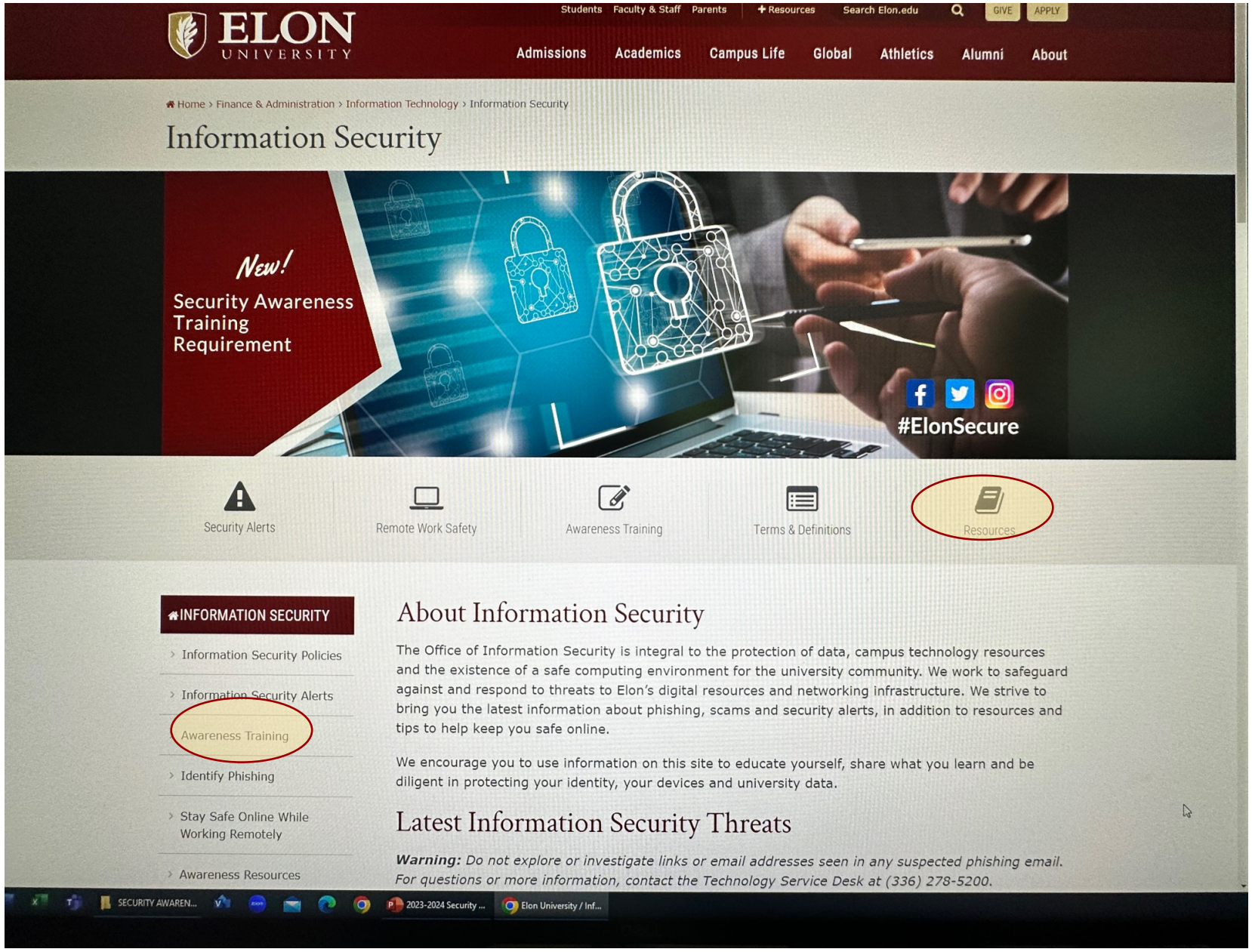


Keeping Safe at Elon – Education & Awareness

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

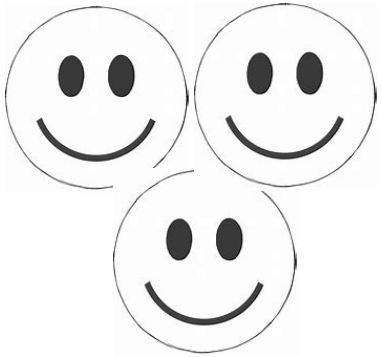


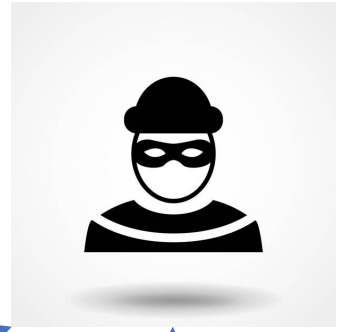
Keeping Safe at Elon – Education & Awareness

LastPass Workshop

Email Phishing

Keeping Safe at Elon – Controls





Log Monitoring
Web Filtering
Application Restrictions
Compliance Controls

Data Loss Prevention

Data Loss Prevention

Multifactor authentication

DNS / IP / App Blocking

IDS / IPS

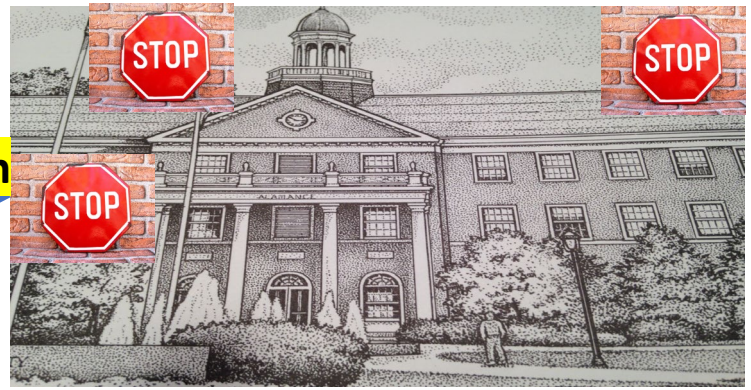
IDS / IPS

DNS / IP / App Blocking

Log Monitoring
Web Filtering
Vulnerability Scanning

Endpoint Controls
Software Updates
Data Encryption
Problem Management
Policies

Multifactor authentication



Security Awareness / Education

ANY QUESTIONS?

To keep our Elon community safe, we focus our efforts on 3 Pillars of Safety:

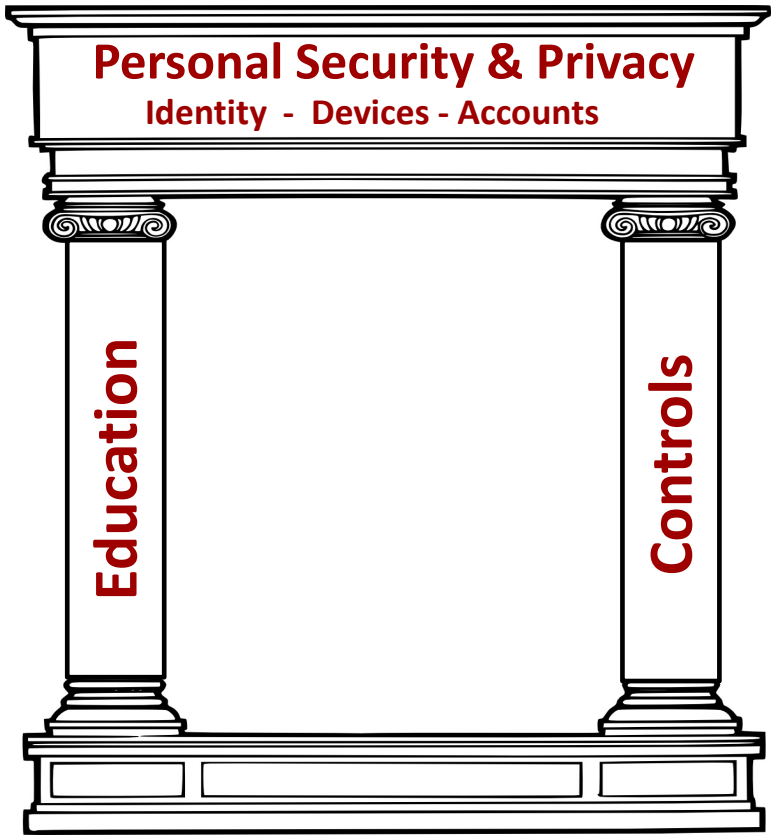
- Policies
- Education & Awareness
- Controls

Keeping Yourself Safe

Keeping Yourself Safe

To keep yourself and you colleagues safe, we should focus our efforts on 2 Pillars of Safety:

- Education
  - Cyber Risks
  - Current Artificial Intelligence (AI) Risks
- Controls:
  - Device Security
  - Privacy

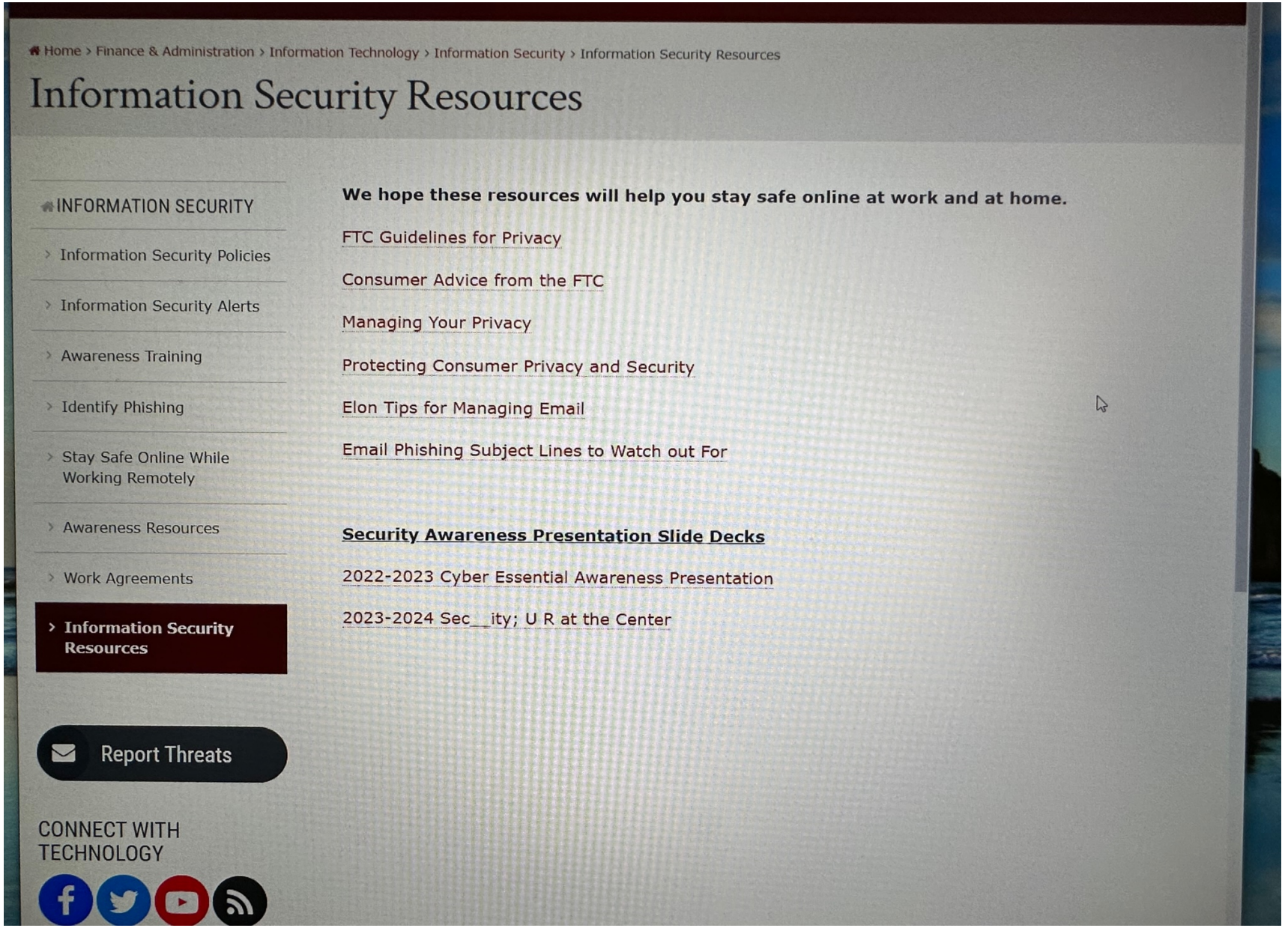


Keeping Yourself Safe - Education & Awareness

Stay Informed

Keeping Yourself Safe – Education & Awareness

Use Elon's Information Security Website to stay informed.



Keeping Yourself Safe – 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.

Are there Real Risks?

1. Consumer privacy & security
2. Biased programming
3. Danger to humans
4. Using AI for destructive behavior
5. Deepfakes
6. Increased and amplified misinformation
7. Unclear legal regulation

Do the benefits outweigh the risks?

Keeping Yourself Safe – Education & Awareness

So – What Can We Do To Protect Ourselves Today?

- Avoid putting/using confidential information into an AI platform
- Don’t be afraid of AI – try it out and keep informed regarding the AI landscape and its capabilities
- 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

Keeping Yourself Safe – Education & Awareness

- In 2020, there were over 10 million active installations of voice assistants in the United States alone.
- In 2023, 35% of companies are using AI and 42% of companies are exploring AI for its implementation in the future.
- By 2024, it's predicted that the global chatbot market will be worth $9.4 billion.
- Currently in Japan, there are hotels entirely staffed by robots and run using AI technology.
- By 2025, it's estimated that the number of IoT devices worldwide will reach 75.44 billion, all of which generate data that can be analyzed with AI algorithms.
- By 2026 the global market size for autonomous vehicles is expected to reach $556.67 billion
- By 2027 according to a report by Gartner, the global AI market is expected to reach $266.92 billion

SC Artificial Intelligence

November 14, 2023 | The most current cybersecurity news involving artificial intelligence

- OpenAI suffered "periodic outages" last week due to distributed-denial-of-service attacks on its ChatGPT services. It was the latest attack in a series of assaults that elevated error rates on its text-to-image model Dall-E on Monday.

- Organizations that use the LLM, either as a business function or as part of a capability from a second party will need to validate **any and all information submitted to and received from the LLM**,"

- It is recommended that all responses be tested and evaluated for malicious software before it's deployed.

- OpenAI reported multiple disruptions this week, culminating in a distributed-denial-of-service attack on ChatGPT on Nov. 8.

Keeping Yourself Safe – Controls: Device Security

- Always run 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)
- Cloud backups – (ensure your device is being backed-up)
- Practice good application security & privacy
  - Beware of malicious apps
  - Grant least privilege for services
  - Review location settings (always-on vs. in-use only)
  - Delete unused apps on mobile devices

Keeping Yourself Safe – Controls: Privacy

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

Smart Devices

Trackers

AI

Camera Technology

GPS

Facial Recognition

Analytics

Keeping Yourself Safe – Controls: Privacy

Privacy Configuration Settings on Mobile Include:

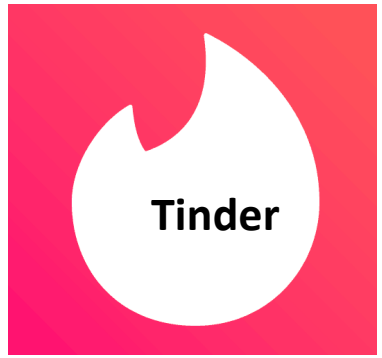
- Location settings / GPS
- Tracking (tracking application use activity)
- Access to your camera
- Access to your microphone
- Access to contacts & calendars
- Fitness / Activity tracking
- Access to your photos
- Access to files and folders
- Bluetooth access
- Access to reminders

Keeping Yourself Safe – Privacy

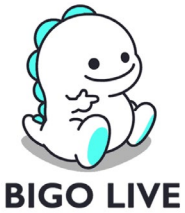
Social Media is the Biggest Risk to Privacy

- Be cautious about what you post in Social Media
- Be careful when accepting “Friend” connections
- Search yourself on Google
- 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

Keeping Yourself Safe – Privacy



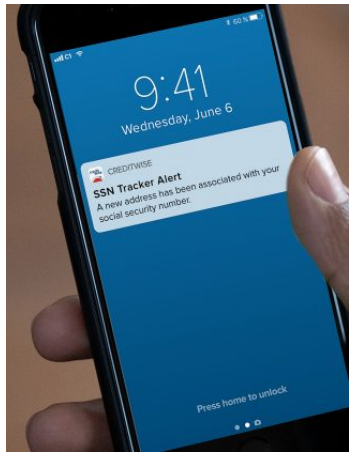
18 Most Dangerous Apps for Children in 2023



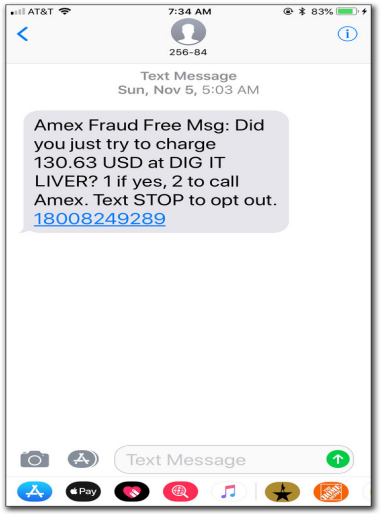
Keeping Yourself Safe – Privacy

- Account Protection / Device Protection
- Home Networks
- Identity Protection Services
- Credit Card Purchase Protection
- Credit Card Fraud Protection
- Credit Monitoring

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

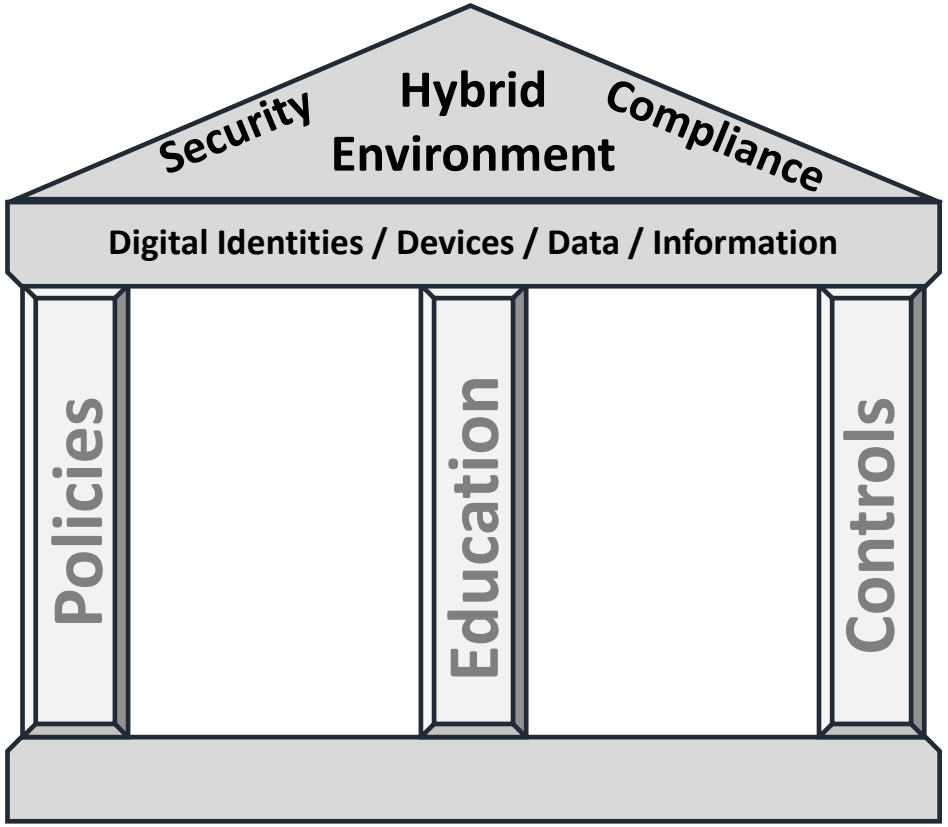


THE HYBRID TECHNOLOGY ENVIRONMENT

Keeping Safe in a Hybrid Technology Environment

To keep us all safe in a Hybrid Technology Environment, we need to work together on focus on these 3 Pillars of Safety:

- Policies
- Education
- Controls



Keeping Safe in a Hybrid Technology Environment - Policies

Policy Requirements:

- Administrative & Technical
  - Policies should address the workplace expectations and responsibilities for the telework workforce.
  - Policies should address technical requirements for supporting a telework/remote environment (i.e.; application, system and device configuration files)

Keeping Safe in a Hybrid Technology Environment - Education

There is always free cheese in a mousetrap.

Don’t get caught in the trap.

Keeping Safe in a Hybrid Technology Environment - Controls

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

Keeping Safe in a Hybrid Technology Environment

#7 – “Personal Information” Security & Privacy

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

Keeping Safe in a Hybrid Technology Environment

REQUIREMENT	DATA TYPES (WRITTEN & DIGITAL)	RESPONSIBILITY
Gramm-Leach-Bliley Act (GLBA)	Student financial information and other non-public student information	Susan Kirkland
General Data Protection Regulation (GDPR)	Personally Identifiable Information for European Union citizens	Christopher Waters
Payment Card Industry Standard (PCI-DSS)	Credit card processing formation – electronic commerce	Gary Sheehan
Family Educational Rights and Privacy Act (FERPA)	Student non-public personal and academic information	Rodney Parks
Health Insurance Portability and Accountability Act (HIPAA)	Medical / health related information for all individuals	Jana Lynn Patterson
State Privacy Laws Personally Identifiable Information (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

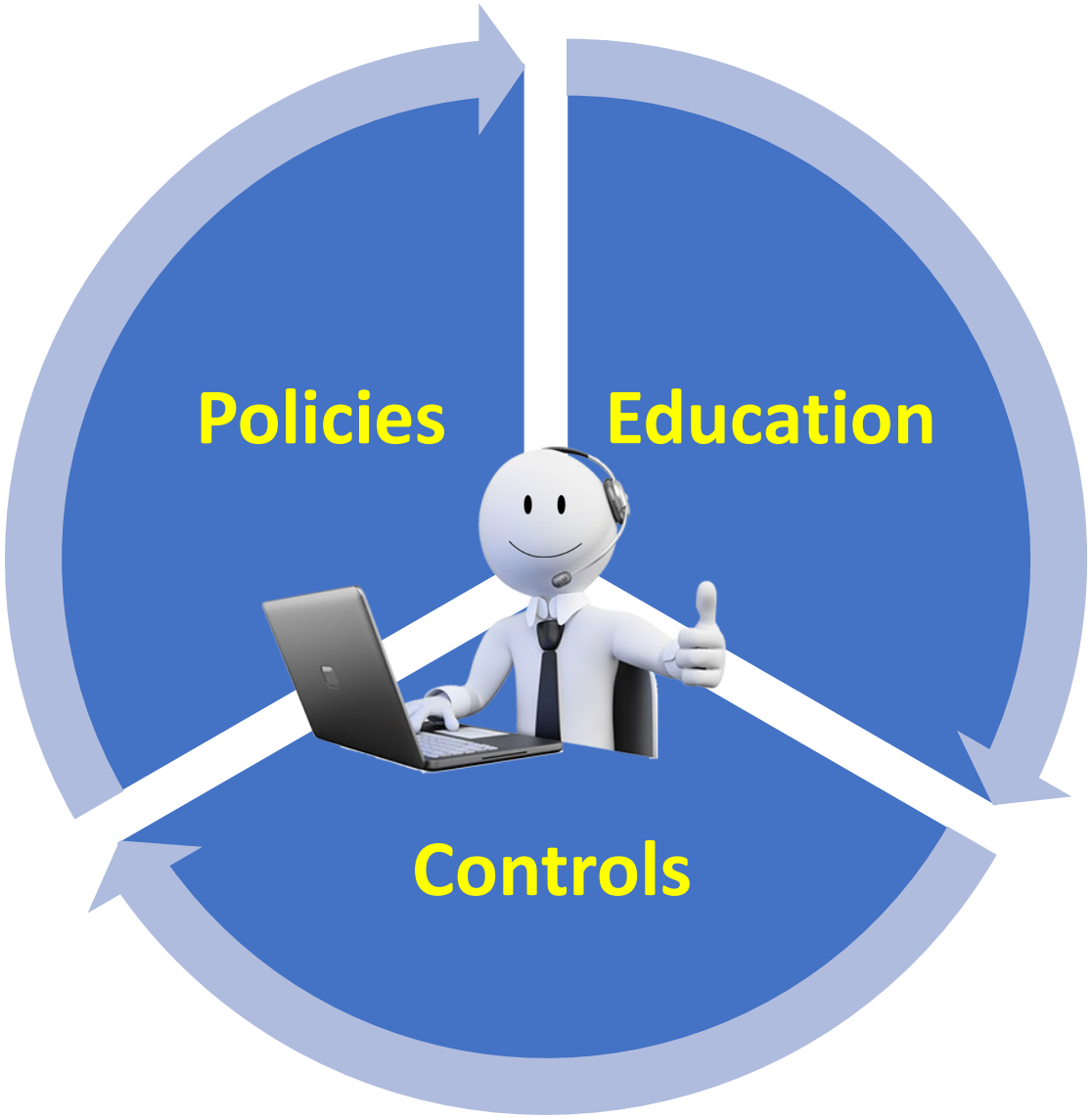
Everyone who handles, accesses, stores, transmits or processes regulated data or sensitive data has a responsibility to be aware of and comply with regulatory requirements.

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 Technology

- Policies
- Education
- Controls



We all must do our part to Ensure Cyber Safety and Data Privacy

Q & A

Feedback is welcome and appreciated. Please complete the survey.