Tips to Keep You and Your Email Safe & Secure

Email phishing remains one of the most effective avenues of attack for cyber criminals – and the biggest cyber risk we experience at Elon. One major factor is due to how sophisticated these types of attacks have become as attackers are now using smarter techniques to trick employees, students and alumni into compromising sensitive data or downloading malicious attachments. Below are several tips that I believe will help keep you and your email safe and secure.

1. Use the ***4S Method*** for checking emails before opening any links or attached document.
    a. Validate the **S**ender of the message.
    b. Examine the **S**ubject line and **S**ubject of the email. There are dozens of typical subject lines scammers use. They also tend to add "urgency for action" within the email body. If the message conveys urgency and threatens consequences if no immediate action is taken, it is most likely a phishing, spoofed or a scam email.
    c. Notice the **S**alutation. Business emails should address you by name and not with a generic greeting.
    d. Review the **S**ignature on the email. Business emails should contain formal signatures. We also encourage all Elon colleagues to use a formal email signature on ALL Elon emails.
2. Elon IT has enabled email labeling for some messages originating from outside our email system. You may see alerts in messages sent from an email address other than @elon.edu. These messages will have "[EXT]" in the title as well as the following header in the message itself, "WARNING: This message originated from outside of Elon University's email system and may contain malicious content." This does not mean that these messages are phishing emails, more a precaution to heighten awareness around responding to them.
3. Don't use your Elon email address to register on personal websites.
4. Use your Elon email address for Elon business communication only.
5. Use encryption (Elon Encryption) when sending emails containing sensitive or regulated data.
6. Do not use your mobile device to send or reply to any email requesting personal, sensitive or regulated data, including your computer credentials.
7. Remember that Elon staff and support people will NEVER ask for passwords or multi-factor passcodes.
8. Use different email passwords for different email accounts.
9. Regarding personal email addresses, like Gmail; Gmail has a built-in "Confidential" mode that allows you to send emails more securely.
10. Be aware of email schemes. Scammers rely on email as their medium of choice for operating schemes because it is cheap, effective and scalable.
11. Investigate suspicious messages. If you receive a suspicious message, you can forward it to infosec@elon.edu where a ticket will be created, and the Information Security Team will investigate the message.
12. When sending private/confidential information (e.g., student academic information), please double-check the recipient to ensure it is correct.
13. Avoid sending any confidential/private/sensitive information to listserv lists.
14. Do not use your mobile device to send or reply to emails that request confidential/sensitive/private information.
15. Please read and comply with Elon's Electronic Communication Policy