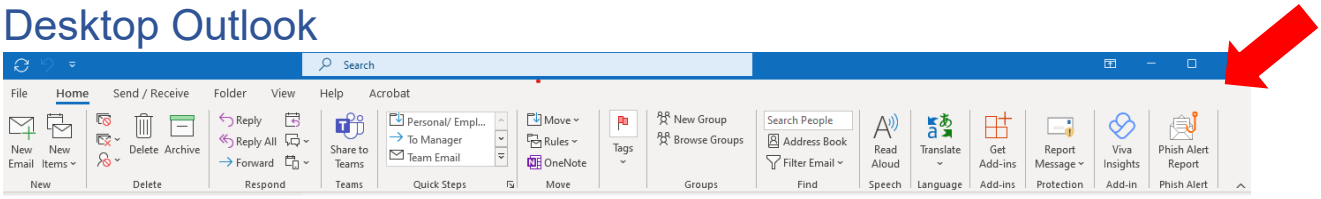
Phish Checker & Mobile Security Checklist

Cybercrimes are an ongoing threat to the security of your data, money, and identity. Cybercriminals can gain access to your networks, computers, devices, and phones if you aren't diligent to watch out for phishing attacks. **Employees who work with protected health information (PHI) are required under the HIPAA Security Rule to maintain appropriate safeguards to ensure the security of PHI.**

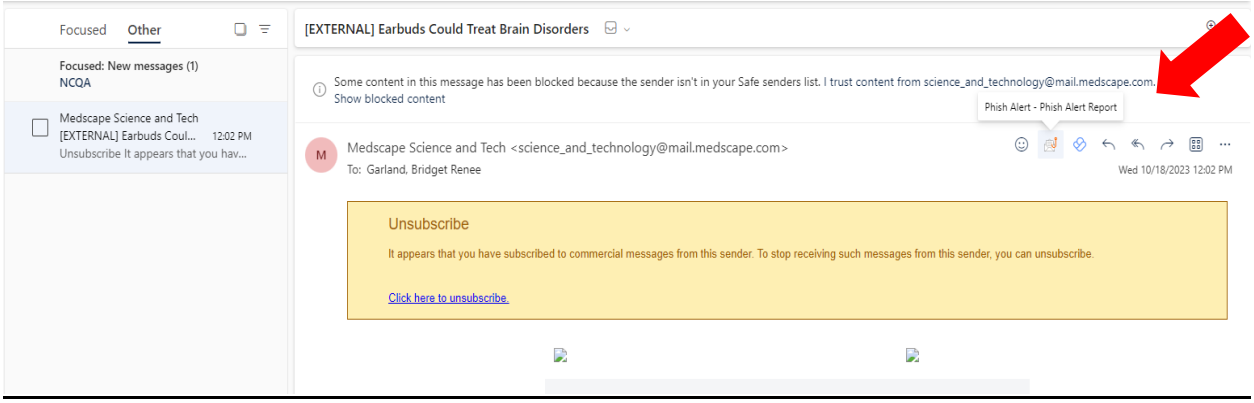
As part of an ongoing effort to protect the security of the ETSU networks, the ETSU Office of Information Technology Services (ITS) has a webpage to assist employees in determining if an email might be a phishing attack.

The webpage provides a list of emails sorted by date and topic which have been identified by ITS as phishing attempts. Employees can report suspicious emails by using the Phish Alert Report button in the Outlook toolbar (as pictured below).

Desktop Outlook



Webmail Outlook



The webpage also lists helpful cyber tips to assist in protecting you, your accounts, and your mobile devices, such as the following:

- never leave your laptop or mobile phone unattended;
- if you find a drive, do not plug it into your computer to identify it, give it to ETSU Public Safety or the HelpDesk;
- avoid accessing sensitive information on public Wi-Fi (Wi-Fi with no password).

Several more tips are listed, and it's worth the time to read through the list as a refresher, especially as employees tasked with securing the PHI of our patients.

If you have questions or need assistance regarding cybersecurity and phishing attacks, you can reach out to the ITS Helpdesk by emailing itshelp@etsu.edu or call (423) 439-4648.
If you have questions about the HIPAA Security Rule, you can visit the ETSU HIPAA Compliance Office webpage or call (423) 439-8533.