Phishing Security

#1 Can't be said enough: be careful where you click and where you put in a password.

#2 Password managers provide significant security from phishing. Please use Lastpass.com or Bitwarden: https://bitwarden.com/

#3 Set up Multi-Factor (or two factor) authentication for all email, social media or other organizational accounts using an app as the 2nd factor like google authenticator. Then for organizations who use Wordpress or similar web-logins that don't have their own two factor solution you can use a tool called SQRL (https://www.grc.com/sqrl/sqrl.htm) for a two factor authentication(2FA). For very high profile or targeted users Yubico(https://www.yubico.com) offers the most secure form of 2FA, which uses a USB like hardware device as the second factor for login.

#4 Https everywhere is a browser plug in or comes in some new browsers and can be used to help enforce server identity assertions. This requires that every site you visit has to make the SSL/TLS lock icon appear.
Get it free at: https://www.eff.org/https-everywhere

#5 Learn how to check SSL/TLS certificates in your browsers window and comparing them to the correct certificates published online and present in your browser. (https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details)

#6 Check Haveibeenpwned.com to see if your current or passed email passwords have been compromised in a breach. Take the Phishing Quiz to learn to spot different tricks used by attackers https://phishingquiz.withgoogle.com/

Constitutional
Communications
concomms.org
@con_comms