

# Cybersecurity Basics

- 1) Use a different Password for each Website.

This may sound difficult but there are some simple ways to do so:

- a) use a Phrase that you can identify with the Website. Examples can be:

Amazon – this is where I shop

Bank: Here I get my Money

Nike: I wear this for Sport

etc etc

- b) use a combination of lower case letters , upper case letters, numbers and special characters.  
This doesn't have to be difficult if you think of a) above and always use the same convention.  
For Nike your Password could be: 1w3ArTh1\$F0r\$P0rT
- c) consider using a Password Manager like 1Password or Dashlane to save your Passwords  
across Devices if you are afraid of forgetting your Passwords

- 2) Never use public Internet without a VPN and never use a free VPN.  
Free VPNs need to make money so they will sell your Data and are thus a security risk.
- 3) Always use two-factor/multi-factor authentication and avoid SMS as Option. If possible, use a Hardware based solution (Chipcard/Fido2 Key) as they are the most secure.
- 4) When setting up your email client, always set the connection security to either STARTTLS or SSL/TLS.
- 5) Set your browser to HTTPS-Only Mode (should be the default but always check).
- 6) Never leave your Phone/Tablet/PC unattended and unlocked if out of your sight.
- 7) Never use public charging cables as they can be manipulated. Better to always carry a Powerbank with you.
- 8) Never open an attachment from someone you don't know or which seems out of place.  
Regardless of what the attachment seems to be.