EMPLOYEE CYBER SECURITY CHECKLIST

DEFEND YOUR DEVICES

- [ ] Keep all software (Including your web browser and mobile apps) updated with the latest releases.
- [ ] Watch out for malicious software. Don't open attachements or click on links in suspicious looking emails, text messages, on social networks, or in random pop-up windows.

PROTECT COMPANY DATA AND ASSETS

- [ ] Don't put confidential information in email, text or instant messages - they may not be secure.
- [ ] Watch out for scams. Never give information like an account number or password in response to a phone call, or email or online request.

CREATE STRONG PASSWORDS AND KEEP THEM PRIVATE

- [ ] Lock your devices and online accounts with strong passwords or PINs. Strong passwords are long phrases or sentences and mix capital and lowercase letters, numbers, and symbols.
- [ ] Use a unique password on each account or device and change them regularly. If you're worried about not being able to remember them, consider using a password manager like LastPass, Dashlane, or 1Password.

USE TWO-FACTOR AUTHENTICATION (2FA) ON YOUR ACCOUNTS

- [ ] Two-factor authentication provides an additional layer of security on top of user passwords.

PROTECT YOUR PERSONAL AND COMPANY DATA ON THE GO

- [ ] Treat all public Wi-Fi networks as a security risk.
- [ ] Encrypt all confidential data on smartphones, laptops, flash drives, and other portable devices in case they're lost or stolen.
- [ ] Never make financial and other sensitive transactions on any device over public wireless networks.

USE FLASH DRIVES CAREFULLY. MINIMISE THE CHANCE THAT YOU'LL INFECT YOUR COMPANY NETWORK WITH MALWARE

- [ ] Don't put any unknown flash (or USB) drive into your computer.
- [ ] On your flash drive, don't open files that are not familiar.

THEFT OR LOSS OF COMPANY DATA OR OTHER ASSETS

- [ ] If sensitive company data or accounts have been compromised because of theft or loss of a laptop, smartphone, or another device, or because of a breach of network security or an account:
  - Report it immediately to IT or security personnel, and to the bank, when appropriate.
  - Change all passwords used to log on to the device.