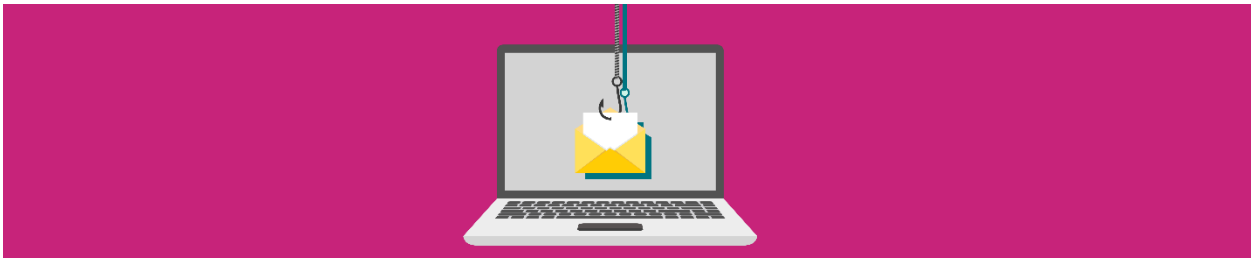
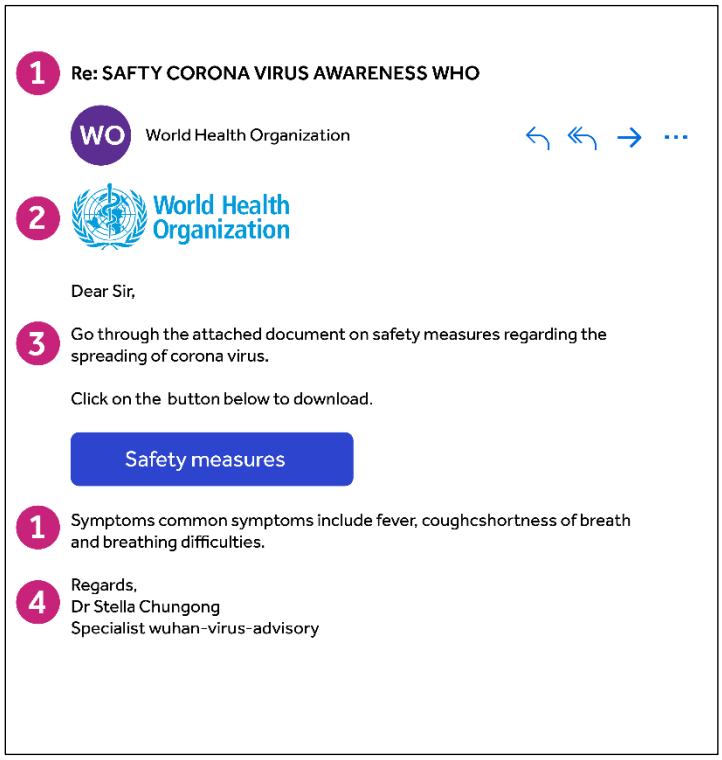
Cyber Security Awareness



Social engineering: phishing, smishing and vishing

Social Engineering is the psychological manipulation of people into performing actions or divulging business confidential or personal Information for the purposes of information gathering, system access, conducting fraud or other criminal activity. Criminals (threat actors) use real life situations e.g. the Coronavirus, to dupe people into providing personal information which they then use for criminal activity and gain.

Fraudsters manipulate victims into providing confidential information or other actions that compromise their security. Phishing involves emails which seem legitimate but direct you to bogus websites or phone lines that capture your personal information. Vishing and smishing are similar techniques where contact is made, respectively, by phone or text.



Examine the following closely:

1 **Grammar/spelling errors:**

Grammatical and spelling errors are red flags indicating this is a suspicious email.

2 **Sender's name:**

attackers are copying images and logos to make emails appear legitimate.

3 **Email tone:**

if outside of the norm of one usually sounds, it's worth a second look.

4 **Email signature:**

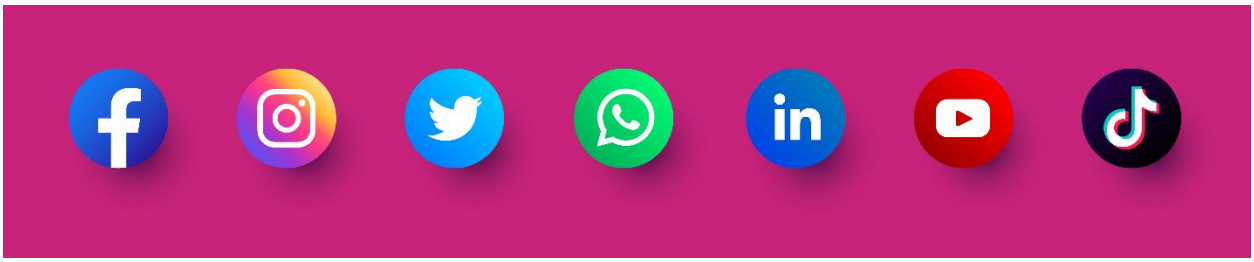
overly generic or doesn't follow company protocols could indicate something is wrong.

How to stay safe

i. Never reveal personal or financial data including usernames, passwords, PINs, or ID numbers.

ii. Be very careful of people or organizations to whom you are supplying payment card information. Remember that a bank or other reputable organizations will never ask you for your password via email or phone call.

iii. Do not open email attachments or readily click on links from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen.



Social Media

Information is shared online via different platforms and is accessible to others. For this reason, it is critical to practice good cyber hygiene to prevent criminals from using your online information (also known as "digital footprint"), making their phishing messages more convincing, to hack into your account and conduct other threats. Even if your account is private, always assume your posts can be shared or seen by the public. Be cautious about publishing personal information that could jeopardize your security, or that of others - for example, your address, current location or contact details.

How to stay safe

i. Accept friend and connection requests only from people you know and can verify.
ii. Ensure any security and privacy settings (i.e., location services, 3rd party apps) are applied to control who can see your profile, information, and posts. Review these periodically and make sure they're updated.
iii. Beware of suspicious links and attachments.
iv. Be aware what your friends, family, and colleagues say about you online, as this can also reveal information that can be used to target you.

Mobile Security

Your mobile devices are always within reach everywhere you go. These devices make it easy to connect to the world around you, but they can also contain a lot of info about you, your friends and family. Contacts, photos, videos, location, health and financial data is all at risk from cybercriminals. It's important to use your mobile safely.

i. Keep your mobile devices and apps up to date - Your mobile devices are just as vulnerable as your PC or laptop. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online threats.

ii. Delete when done - Many of us download apps for specific purposes, such as planning a vacation, and no longer need them afterwards. It's a good security practice to delete all apps you no longer use.

iii. Secure your devices - Use strong passwords or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.

iv. Get savvy about Wi-Fi hotspots - Public wireless networks and hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected. Limit what you do on public Wi-Fi and avoid logging in to key accounts like email and financial services on these networks.

v. Now you see me, now you don't - Some stores and other locations look for devices with Wi-Fi or Bluetooth turned on to track your movements while you are within range. Disable Wi-Fi and Bluetooth when not in use.

Using Business Communications

Business communications tools such as email, and instant messaging (IM) are vital but using them in the wrong way carries the risk of significant reputational damage and information asset leakage.

i. You must use the Information Labelling Tool (ILT) to label all Information with its correct handling label

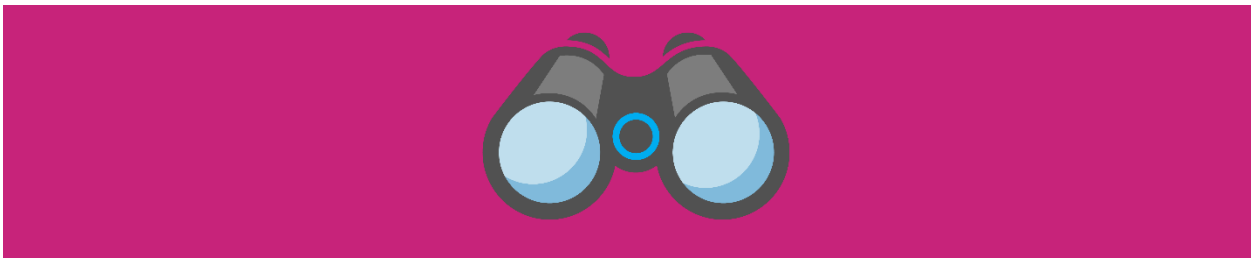
ii. You must take reasonable steps to avoid accessing or introducing malware (such as viruses) or inappropriate content (such as pornography) - for example, avoid opening suspicious attachments or clicking on links in suspicious emails.

iii. You must ensure that people to whom you send Information are authorised to receive it.

iv. If you don't want to receive messages from a particular individual or organisation you might be able to 'block' them.

v. Email service providers can often identify spam emails also known as junk emails. These are usually unwanted emails sent out in bulk trying to sell you something. Your email account will probably have a 'junk/spam' folder.

Sometimes legitimate emails can arrive in this folder, so it's worth checking it regularly to move ones you want to keep and deleting emails that you're not interested in, and blocking them from sending any more.

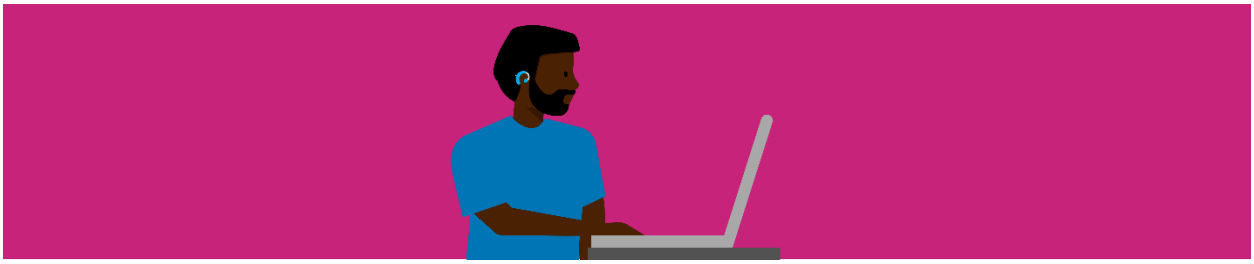


Data Security and Privacy

Personal information is valuable hence consider taking the following actions to create a culture of respecting privacy, safeguarding data.

Maintaining your privacy

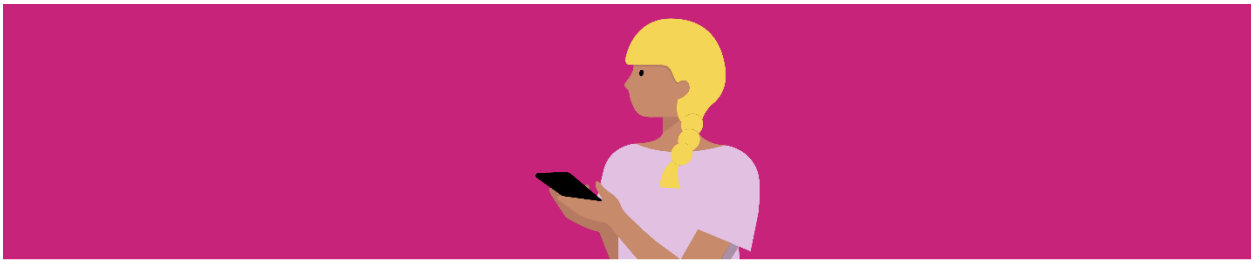
i. Ensure you always have effective and updated antivirus/antispyware software running.
ii. In a public or work environment, check your computer physically for any unusual devices that may be plugged in, especially on the keyboard cable
iii. Store personal and financial documents securely
iv. Shred unwanted personal or financial documents
v. Be cautious about who is trying to befriend you online including via email and social networks/dating sites.
vi. Use secure websites when shopping or banking online
vii. Use strong passwords, change your passwords regularly and never reveal them to other people



Working Securely

Whether you're working remotely – from home or in public – there are risks and you must ensure that Information is handled, protected and secured.

i. Log off or lock your computer when leaving it unattended.
ii. Don't leave devices or Information on display or unattended and be mindful of who can overhear your conversations.
iii. Physical and electronic Information must be correctly labelled, shared (emailed, printed, posted, faxed) and stored to ensure the appropriate Information Security controls are applied.
iv. Ensure you work in a secure location where you can protect your information. Avoid working in busy public places such as coffee shops or on the train when commuting.
v. Work in a space that is private. If you're having conference calls or video meetings, be aware of whether other people might be able to eavesdrop on what is being discussed, even inadvertently.

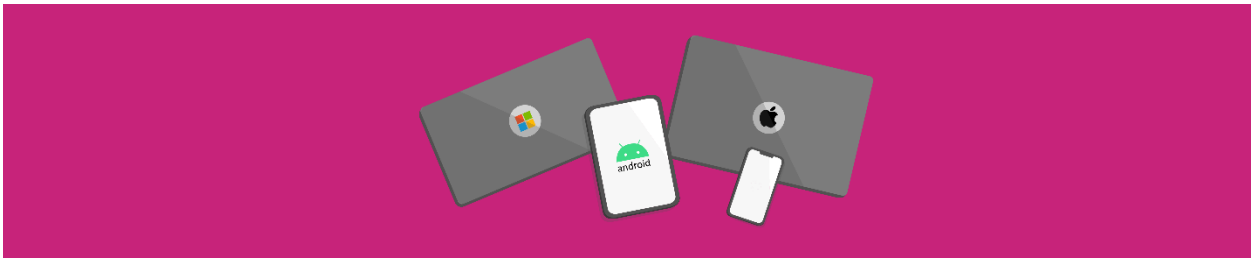


Securing Financial Transactions

Even though there are many benefits to online banking, there are also some risks involved. Online accounts are also the target of criminals.

Banks and other financial institutions never ask their users to provide any sensitive or personal information via email or phone call. Cybercriminals might convincingly copy the formatting, language, and common phrases of legitimate banks.

i. Buy from secure websites for Online Financial Transactions – Ensure that the site have an SSL Certificate and a certificate of authentication. Please check some reviews on the internet before proceeding further with the transaction.
ii. Always log out after accessing your shopping or banking accounts, then close your browser. Don't allow your computer to store your usernames and passwords for shopping and banking sites.
iii. Choose a strong password filled with numbers, symbols, and lowercase/uppercase letters.
iv. Always keep up-to-date antivirus and firewall security programs. Scan your computer frequently and check to make sure your firewall is turned on before shopping online, paying bills, or accessing your bank accounts.
v. If something looks suspicious, get offline and shut down your computer immediately. Trust your instincts.
vi. Don't use one-click or easy-pay payment options. Make sure every transaction requires your password.
vii. Don't use public Wi-Fi when performing online transactions. Do your shopping at home, from your own computer.



Securing ICT (Information Communications Technology) Systems

Below points outline the precautions to be taken while securing ICT (Information Communications Technology) systems.

i) **Keep your mobile devices and apps up to date:** having the most up-to-date security software, web browser, operating system and apps is your best defense against viruses, malware and other online threats.

ii) **Secure your devices:** use strong, complex passwords or touch ID features to lock your devices. These security measures can help protect your information if your device is lost or stolen and keep prying eyes out.

iii) Kindly ensure that your system has latest antivirus definitions and latest O.S. patches and application updates installed.

iv) Limit what you do on public Wi-Fi and consider using a **virtual private network** (VPN) or a **personal/mobile hotspot** if you need a more secure connection on the go.

v) **Install antivirus**: protect your smartphones in the same way you would your personal computer with antivirus software.

vi) Disable Wi-Fi and Bluetooth when not in use to avoid your location being tracked without your knowledge by nearby devices.

vii) Do not store any secret or sensitive information on the collaboration tools like JIRA, Confluence etc.

Using IT Systems and the Internet

IT Systems and access to the Internet are powerful resources which support a large number of business activities. They are also sources of many threats. Here's what you must do to help protect yourself when you use IT Systems and when you access the internet:

Fraud and Scams have been around for hundreds of years, but what has changed over time is how criminals operate. Technology has made our lives much easier, but it's also made it much easier for those trying to steal our personal information and our money. Firstly, let's consider what we mean by Cybercrime.

The words 'Fraud' and 'Scam' are often used interchangeably which could imply they mean the same thing but in fact this is not the case.

Fraud is a transaction which the customer does not recognise, has not made themselves or didn't authorise.

A scam is where you're tricked into making or authorising a payment to a criminal's account. Scammers impersonate banks, retailers and official organisations using emails, phone calls and texts that look and sound genuine.

Share this guide with any joint account holders so they are aware of potential risks.

We are here to help - If you think you have fallen victim to a scam or fraud, please contact us immediately: **+91 22 6000 7888** / **customerservices@barclays.com.**

Received a suspicious email? Forward it to: **internetsecurity@barclays.com**, then delete it.

Visit: https://privatebank.barclays.com/support-and-information/security/