HSBC UK | Opening up a world of opportunity

Cybersecurity made simple

Document sharing

- Use shared drives / SharePoints where possible
- Use encryption / passwords when dealing with sensitive documents
- Avoid printing unless absolutely necessary

Common features of phishing emails

Too good to be true

Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately.

Sense of urgency

A favourite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time.

Hyperlinks

Hovering over a link shows you the actual URL where you will be directed upon clicking on it.

Attachments

If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it!

Unusual sender

Check the spelling of the sender's email address e.g. xxx@hsbc.com compared to xxx@h5bc.com.

To

Were you copied in on an email sent to one or more people, but don't personally know the other people it was sent to?

Did you receive an email that was also sent to an unusual mix of people? For instance, it might be sent to a random group of people at the organisation whose last names start with the same letter, or a whole list of unrelated addresses.

Cybersecurity

A short guide on response and recovery

Small Business Guide: Response & Recovery

Top 5 things you need to **STOP** doing on your mobile phone now!

1. STOP turning off auto updates for operating systems and apps!

Keep Operating Systems (OS) and apps patched and up-to-date. It is the easiest way to protect data.

2. STOP using weak or non-existent device lock & passwords!

Complex passwords or passphrases protects both prying eyes in general and access to files and your data.

3. STOP clicking links in email OR social media OR unknown senders!

Social media phish is a very effective way to trick users. If in doubt - don't click!

4. STOP downloading apps outside Apple and Google stores

There are tons of fake apps posing as real and legitimate apps. Use only official app stores!

5. STOP connecting to random Wi-Fi hotspots!

It is best you either know the Wi-Fi you are connecting to, or use a VPN on your device.

For Intermediary use only.

HSBC UK Bank Plc. Registered in England & Wales with number 09928412. Registered Office: 1 Centenary Square, Birmingham, B1 1HQ, United Kingdom. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our Financial Services Register number is 765112. ©HSBC Group 2022. All Rights Reserved.

This document is intended for reference and illustrative purposes only. It does not constitute an offer or advice from HSBC UK. Whilst HSBC UK will try and ensure that the information contained in this document is complete and accurate at the date of publication, it cannot guarantee this and therefore it makes no representation or warranty as to the accuracy of the information. HSBC UK accepts no liability for any direct, indirect or consequential losses or damage of any kind suffered by you, your employees, agents, contractors and sub-contractors or by any of your customers arising from the use or reliance on the information contained in this document and as such liability is excluded to the maximum extent permitted by law.

Maintaining appropriate IT security protocols and customer protections from phishing attacks or other cyber risks is the sole responsibility of each broker firm/authorised intermediary. For further advice on any IT security issue or cyber risk, please speak to your IT department/Phishing team.