Current local and international scams

There are thousands of types of scams today, but most boil down to stealing money, property, or information. Below is an overview of common scams.

Some common scams

Phishing

Receiving an e-mail from someone pretending to be your bank official indicating you are overdrawn or made a purchase that you didn't make and asking you to log in and verify the information. However, the link in the e-mail directs to a fake site that logs your username and password information. So please be mindful when clicking!

Donation scam

A person claiming, they have a child or know someone with an illness and need financial assistance. Although these claims can be real, many people create fake accounts on donation sites to scam people out of money.

Telephone Scams

Telephone scammers try to steal your money or personal information. Scams may come through phone calls from real people, robocalls, or text messages. Callers often make false promises, such as opportunities to buy products, invest your money, or receive free product trials. They may also offer you money through free grants and lotteries. Some scammers may call with threats of jail or lawsuits if you don't pay them.

Threat scam

Someone sends an e-mail claiming to work for a company that found something wrong with you or your company and is threatening legal action unless you pay. Often these scams can be quickly identified because they're asking for Cryptocurrency as the form of payment.

Catfish

A person who creates a fake online profile to deceive someone. For example, a woman could create a fake profile on an online dating website, create a relationship with one or more people and then create a fake scenario that asks others for money. Always be mindful on whom you are talking with.

Online survey and lottery scams

Online survey scams are survey sites that say they offer money or gift vouchers to participants and Prize scammers try to get your money or personal information through fake lotteries, sweepstakes, or other contests. Many claim that you've won a prize but must pay a fee to collect it. Others

require you to provide personal information to enter a "contest." These scams may reach you by postal mail, email, phone call or text message.

1. Dating site/Dating app scams

- Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions.
- They then suggest chatting privately outside of dating websites or apps e.g. social media/email. Often, what they tell you in private does not match their public profile.
- These scammers play on your emotions to get you to provide money, gifts or personal details.
- Many times victims are too embarrassed about their loss to report the crime.
- They work to gain your trust (sometimes over several months) and then tell you an elaborate story asking you to provide money, gifts, or personal details such as bank account or credit card details.

2. Remote access scams

- Criminals might reach out to you posing as a legitimate business or provider, often claiming to be there to protect you from fraud or scams.
- They create a feeling of urgency and danger to try and get you to do things that could compromise your bank details so they can steal money from your accounts.
- A fraudster calls, impersonating your internet provider. They tell you that you have some connection problems or your bill is overdue and while on the line they may request remote access to your computer.
- Then has the opportunity to steal your banking details and move money out of your account or convince you to transfer funds to a false account.

3. Investment scams

- Investment scammers cold call, email or reach out to people via social media to offer them once-in-a lifetime or extremely rare investment opportunities.
- They'll often sound very knowledgeable and make you feel the investment opportunity is too good to miss out on.
- Scammers are likely to ask you to invest more money or make a tax payment in order to allow the release of your funds.
- Typical scam investments involve property projects, share and stock promotions, binary options, foreign currency trading and cryptocurrency (ie: Bitcoin).
- Always be wary of 'investment opportunities' that promise a high return with little risk.

4. Prize & Lottery related scams.

- You will receive notification/Pop ups that you have won a lot of money or a fantastic prize in a competition, lottery or sweepstake that you don't remember entering. The contact may come by mail, telephone, email, text message or social media.
- The prize you have 'won' could be anything from a tropical holiday to electronic equipment such as a laptop or a smartphone, or even money from an international lottery.
- To claim your prize, you will be asked to pay a fee. Scammers will often say these fees are for insurance costs, government taxes, bank fees or courier charges.
- The scammers make money by continually collecting these fees from you and stalling the payment of your winnings and collecting your credentials.

5. HSBC Staff recruiting Scam

- Individuals have been reaching out to others (especially in rural areas) claiming that HSBC is recruiting staff.
- In order to start the hiring process a fee needs to be transferred to that individuals account number.
- They will promise or give you fake documents to prove who they are and what they will give you after you do the payment (mobile phone, motor bike).

How to spot and protect yourself from scams

Simply the scammers might get in touch by phone, email, postal mail, text, or social media. Protect your money and your identity. Don't share your personal information. Please follow below guidelines to protect yourself from scammers.

1. Stay on top of things

- Check your bank accounts and statements regularly, and keep an eye out for any unfamiliar transactions.
- Get a copy of your credit report once a year and check it for any unusual activity. If a fraudster has used your name to take out a loan or credit card, it may not show on your regular statements.
- Set up Account Alerts via HSBC Online Banking so you can be instantly notified when specific transactions take place.

2. Always question unexpected messages

- Whether or not you were expecting the message, make sure the person contacting you is actually from the company they say they're from – don't just take their word for it.
- Never automatically assume an email, text or phone call is authentic. Be a sceptic.
- Criminals can falsify phone numbers and pose convincingly as bank employees or other trusted officials.

- They'll try to trick you into revealing security details by telling you you've been a victim of fraud.
- If you have any doubt at all, get the caller's name and contact information and hang up. Then, contact the company directly, using an e-mail or phone number that you know for sure is genuine, for example from the company's website.
- Always look carefully at links, e-mail attachments and suspicious texts before clicking on anything. Don't open from sources you can't verify as safe and genuine. If in doubt, delete the email or SMS immediately.

3. Never disclose personal information

- A bank will never ask you for your PIN or full password in an email, on the phone or in writing.
- Protect your HSBC SMS code like you would your password and PIN.
- Never download or install software you're not familiar with or allow a person making an unsolicited call to access your computer remotely.

4. Don't be pushed into making any important decisions

- A bank or other trusted organisation will never force you to make an on-the-spot financial transaction or transfer, or rush you while you pause to think.
- Slow down, so that you can consider your actions and your options. If you're uncomfortable in any way, don't be afraid to hang up.

5. Trust your instincts

- They don't call it a gut feeling for nothing. If something feels wrong or seems too good to be true, question it.
- Always make it a point to think carefully about the information you're giving and the decisions you're being asked to make.

6. Make sure it's secure

- If you shop online, always use secure websites. Make sure the web address (URL) starts with "https" or has a padlock symbol at the front.
- Do not save your card details on your web browser.

8. Reduce risks of card fraud

- Always check the amount you're paying has been entered correctly. Always go for the more secure options of inserting or tapping your card, or even using a PIN.
- Don't share your PINs or passwords and don't write them down anywhere – if you forget them, you can always call the bank for assistance.
- Use strong passwords consisting of letters, numbers and symbols, and change them regularly.
- Always update your computer, tablet and smartphone operating systems as soon as these become available and install anti-virus software.