Staying safe online

To help protect our customers during the COVID-19 pandemic, we're encouraging everyone to take advantage of our online and telephone banking services, instead of visiting branches.

However, it's important to be extra vigilant about security in these times. Unfortunately, fraudsters are using the COVID-19 outbreak as an opportunity to carry out new scams by email, calls and texts, in their efforts to retrieve personal banking information.

To help you keep your accounts and identity secure, we've collated some useful tips to help you stay safe when banking online.

1

Be vigilant with ANY calls, texts or emails claiming to be from your bank

Remember, while your bank may ask security questions to confirm your identity, they will NEVER ask you to:

- Share your full password, security number, or other security details.
- Share your PIN code, expiry date and CVV (3 digit number on the back of your bank card).
- Transfer money between your own accounts or to another account (without your prior instructions).

Any email, text, call, or visitor that asks you for any of the above information is likely to be fraudulent.

A common trick employed by fraudsters is to ask you to click on a link in an email, which takes you to a website that resembles your bank's. If you enter your login details into this lookalike site, they can be stolen by the fraudster, and used to access your money.

The best way to avoid this is to always search for your banking website through your web browser, rather than clicking on links in emails. You should also be especially careful of emails, texts, and calls asking for overdue payments, or offering refunds/prizes.

If you are ever in doubt that you are speaking to a genuine member of staff, don't hesitate to hang up. You can then check if the communication was legitimate by contacting your bank, using the details on your card or on their official website.

2

Update your online and mobile banking passwords

Unfortunately, these unprecedented times do not deter hackers and identity thieves. So it's still important to regularly update your banking passwords, to prevent fraudsters from accessing your accounts. Remember to make your passwords as unique and strong as possible by:

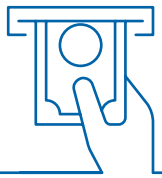
- Using a combination of letters, symbols and numbers in your password.
- Avoiding commonly-used information that can easily be linked to you. E.g. pet names, partner's name, date of birth, place of birth etc.
- Using phrases or acronyms instead of single words.
- Making sure your new password is completely different to your old one. For instance, changing 'Bank1' to 'Bank2' would not be very secure.
- Never using the same password for other accounts/services.

3

Keep a regular eye on your account

Checking your bank statements each month can help you to spot any unauthorised transactions. Online banking gives you even more control, and you can check your account 24/7.

Often fraudsters initially make small transactions to 'test the water' before stealing larger amounts. So if you notice any irregularities or unusual activity not authorised by you, contact your bank immediately.



4

Enable mobile banking and online banking alerts

Working from home does not necessarily mean you have more time on your hands. Many of us still have to balance other responsibilities including childcare, household chores and caring for our loved ones. As a result, we may not have the time to log into our online banking as frequently as we would like to.

With UBL UK online banking alerts, you can arrange to receive email or SMS notifications whenever there is new activity on your account(s), such as:

- Unsuccessful login attempts
- Personal information updates
- Password updates
- Daily balance tracking
- Wire transfers
- Transaction alerts (for all transactions or above a specified amount)

Enabling alerts on your account(s) can not only help you save time, but also promptly identify any unauthorised activity on your account. You can then immediately report this to your bank, and hopefully stop the fraudsters in their tracks.

5

Consider using a Virtual Private Network (VPN)

As a result of the COVID-19 outbreak, many individuals worldwide are now required to work from home. Lots of internet providers have since established free Wi-Fi hotspots, particularly in major cities like London.

You should never use public Wi-Fi to access online banking. However, if you live near a public hotspot or are reliant on 'pay as you go' Wi-Fi networks, you could try using a Virtual Private Network (VPN) to log on.

A VPN creates a secure, hidden connection between your computer and the internet, helping to prevent potential fraudsters from intercepting your communication with a website. There are a number of free VPN tools available. Alternatively, web browsers such as Google Chrome have a similar option called 'incognito mode', but this should only be used when absolutely necessary.

We hope you find the tips listed above useful. Please always be aware of criminals who may be trying to take advantage of this unprecedented period. If you think that any fraudulent activity or unauthorised transactions may have taken place on your account(s), do not hesitate to contact your bank.

Stay safe. UBL UK.

UnitedBankUK @UnitedBankUK

UBL where you come first