**Press Release**

# Ulster Bank Shares Useful Tips on Fraud and Scams, Building on Existing Supports and Services

**07 September 2020:** Ulster Bank is today reminding customers to be vigilant against fraud and scams, including Smishing or text message scams, and is sharing tips aimed at protecting people, while providing support and information about the dangers of handing over sensitive personal details to people they don't know.

It follows an increase in the volume and nature of financial fraud and scams in recent months, as criminals target people who are working, shopping and banking more online due to coronavirus.

Commenting, Ulster Bank's Managing Director of Personal Banking, Ciarán Coyle, said:

> *"Coronavirus has changed all our lives and we're doing lots of things differently as a result, including shopping, working and banking more online. That's why we're asking people to be extra vigilant. Scammers are smart and they change tactics all the time. No one should feel embarrassed if they think they have been scammed because we are all susceptible to it, depending on how sophisticated the scam is. This is one of the reasons why we're asking people to contact us immediately if they think they have been the victim of a scam and to share their experience with their friends or family."*

The bank's Community Protection Advisor Denise Cusack outlines the most common fraud and scams and advises people on how they can avoid them:

> *"Ulster Bank (or any financial institution) will never ask you for your online banking login details, full password or PIN. Never disclose your banking details to a third party and if you receive a request for this information, whether it's over the phone, in person, by email or by text message, refuse immediately and call us using the number on the back of your card, or a number you trust. Similarly, if you receive a communication claiming to be from your bank, asking you to move your money for fraud reasons, you should decline this immediately. Your bank will never ask you to do this*
>
> *"Businesses also need to be vigilant. Invoice re-direction fraud has become more common, and occurs when a business receives a fraudulent email claiming to be from an existing supplier, advising of new bank details for payment. Oftentimes, these requests look like they're coming from an email address or name that you recognise. One of the best ways to figure out if a request like this is genuine is to pick up the phone to your supplier directly, using a number you trust."*

Ulster Bank has a wide range of anti-fraud and scams supports and services. The bank analyses payments for irregularities and communications from a customer's computer or mobile app when using online or mobile banking are encrypted. In addition, regular tests of its banking systems are undertaken by independent industry experts to ensure that the services meet the highest standards of security, while all of Ulster Bank's websites are monitored and protected from sophisticated attacks.

Customers receive enhanced scam warnings when transferring money to new beneficiaries in their mobile app and online banking services and can report any suspicious activity by ringing the phone number on the back of their debit card.

Ulster Bank also helps customers to protect themselves with tips on staying secure and free tools for extra protection. The bank has formed a partnership with the antivirus company Malwarebytes to offer their product Malwarebytes Premium to all its customers free-of-charge until May 2022. This will protect whatever device they are using by detecting and removing viruses and other malware, and blocks scams phishing for customer details.

The bank's online Security Centre is a one-stop-shop for security information for customers. This includes the 'Friends Against Scams' initiative to help prevent people from becoming victims of scams and suffering from the emotional and financial impact. It provides information to customers and encourages them to have conversations with friends, family, and the community so we can all help each other spot a potential scam, report it, and share our knowledge.

You can find out more information by visiting https://digital.ulsterbank.ie/personal/security-centre.html

**ENDS**

**NOTES TO THE EDITOR**

## Ulster Bank's top tips to protect yourself from Fraud and Scams:

1. **A genuine bank will never contact a customer to ask for their full PIN or password.** Stay in control and have the confidence to refuse unusual requests for information. Your bank will never ask you to disclose card reader codes over the phone under any circumstances.
2. **A genuine bank or organisation will never ask a customer to transfer money** to a safe account for fraud reasons. If you're asked to do this, you can be confident it is a scam.
3. **Be vigilant.** Just because someone knows basic personal details (such as names and addresses or even a customer's mother's maiden name), it doesn't mean they are genuine. We advise customers to listen to their instincts – if something doesn't feel right, take a moment to stop and pause and think things over.
4. **Customers should always follow their bank's security advice** and should never download software that enables someone to remotely access their device, especially following a cold call.
5. **Customers should be cautious with what they disclose on social media** and take precautions to ensure that their profile is private and only viewable to people they know.
6. **We advise that customers should keep their mobile devices' operating systems up to date** to ensure that they have the latest security patches and upgrades.

**ENDS**