

S C A M

FRAUD PREVENTION POLICY

“

We are working hard and relentlessly to protect you against fraud but we cannot do it alone.

There are several other ways you too can protect yourself and we have carefully outlined different types and how you can as well protect yourself.

”

We all think fraud is something that happens to other people, until it happens to us.

The fact is, we are all equally susceptible but, in our beliefs, we are better protected when we stick together as a team and family and work together to put an end to fraudulent activities which are targeted towards our accounts.

Aufin bank has been working tirelessly, developing tools and techniques that make banking safer, trustworthy and worthwhile experience but it seems not enough. We need your assistance. If we all work together and follow a few simple steps, we can be better protected and keep your investments safe and that is good for everyone.

HOW YOU CAN PROTECT YOURSELF

Update Your Passwords

Try to change your account passwords at least, twice a year. Do not use a password that can easily be guessed and make sure that your online banking passwords, as well other passwords related to your accounts are not the same as the ones you use for other websites.

Always Question Unwelcomed Approaches

Instead, contact us directly through any available means using an email or phone number that you can confirm its authenticity.

Never Share Personal Information

Never reveal your password or share your card details over email. Be careful with the level of details you share on social media websites, third party public domains and do not forget to check your privacy settings.

Stay Safe Online

Always update your computer or your cellphone device or tablet operating systems as soon as they become available and also, install your antivirus software.

Shred Important Documents

Shred any paperwork which the bank must have issued you over email in any case you print it as they may contain sensitive data or information which if in wrong hands, may jeopardize the safety of your account.

FORMS OF SCAM

Email Scams – Email scams or phishing refers to when a fraudster sends you an email, encouraging you to share personal details or to click on fake links. Take a few minutes for a better look to check whether the email seems genuine or not.

Clicking on a fake link may result in you being targeted in different ways, like a phone call from your bank's fraud department or more juicy offers.

For instance:

- An email saying you are owed a refund or
- You won a lottery you never entered for or
- Telephone preference service coercing you to pay for a lifetime subscription.

Text Scams – Text scams or smishing refers to when a fraudster sends you a text that appears to be from your bank or in some cases, from another organization that you trust. They may tell you that there is being a fraud on your account and ask you to share or update your personal information or details.

The text may offer vouchers, a tax refund or ask you to confirm the delivery of a parcel.

For instance:

- A text telling you that access to your account has been restricted and further demanding you provide your details through a link to reinstate access or
- A text asking you to transfer your funds to a different destination, usually tagged as a "safe account".

Online Scams – This form of scam is on the rise currently. Fraudsters use sophisticated means to gain access to your banking information, creating bogus links and retailer web pages as well as fake pop-ups.

You must protect yourself by:

- Always updating the operating systems of all the device with which you use to access your account as soon as they become available.
- Install anti-virus software on all your devices.
- Do not enter sensitive information on untrusted third-party domains.

Other forms may include but not limited to:

- Romance Scams.
- Investment Scams.
- Account Takeover Fraud.
- Email Interception Scams.
- CEO Fraud.



Whichever information which you may receive through either email, calls or text, through any medium, please do endeavor to communicate with your assigned account manager if any or directly to our customer service out let on our official website - www.aufinbank.com

No matter how urgent it may seem, always take the time to validate any request made of you through any medium with us.

