Europe Arab Bank

Fraud Bulletin – Keeping Our Customers Safe

March 2020

Contents

1 Protecting you against fraud

We are all operating in uncertain times and Europe Arab Bank would like to let you know how we are working together within the Bank to keep you safe from fraud by outlining things to look out for, that we would never ask of you.

Fraudsters may try to imitate our branding or have web pages that look like ours. Here are some tips and guidance should you feel uncertain of whether any contact from us is not legitimate.

1.1 Here are some key things to remember:

- A GENUINE BANK OR ORGANISATION WILL NEVER CONTACT YOU OUT OF THE BLUE TO ASK FOR YOUR PIN, PASSWORD OR TO MOVE MONEY TO ANOTHER ACCOUNT.
- NEVER CLICK ON A LINK IN AN UNEXPECTED EMAIL OR TEXT – *you could be giving someone access to your personal and financial details.*
- ALWAYS QUESTION ANY CALLS FROM A BANK OR A COMPANY YOU WEREN'T EXPECTING IN CASE IT IS A SCAM. IF YOU ARE IN DOUBT, TERMINATE THE CALL – *You can contact them using a different method if you want to check if it was a legitimate call for instance, if they email, you call them, using an email or phone number you know is legitimate.*
- DON'T ASSUME AN EMAIL OR PHONE CALL IS AUTHENTIC – *just because someone knows your basic details (name, address, or mother's maiden name) it doesn't mean they are genuine.*
- DON'T BE RUSHED INTO MAKING A DECISION OR A FINANCIAL TRANSACTION ON THE SPOT – *Europe Arab Bank – or any trusted organisation would never do this.*
- LISTEN TO YOUR INSTINCTS – *if something feels wrong then it generally is.*
- TAKE TIME TO THINK ABOUT WHETHER THIS IS GENUINE OR IF IT COULD BE AN ATTEMPTED FRAUD – *your vigilance will be appreciated by genuine organisations and ourselves at Europe Arab Bank.*

2 Frauds that directly target you

2.1 Fraudsters contacting you directly:

- By impersonating us (Europe Arab Bank) through emails, and asking you to click on links or entering your personal details (Phishing) – *we will never ask you to enter any of your personal details or click onto links within an email*.
    - If this happens, then call your Relationship Manager/Director by phone, and talk to someone you recognise.

- By sending you phone calls or voice messages, and then try and persuade you to transfer funds – *we will never ask you to transfer funds in this way.*
    - You have your dedicated Relationship Manager/Director, who you know. If it is not someone you know, hang-up and contact your Relationship Manager/Director by email.

- By sending you a text message asking you to click on links or download information – *we will never ask you to click on links within text messages or ask you to download something onto your phone*.
    - If this happens, email us or call us using your telephone landline, and speak to your Relationship Manager/Director.

2.2 Fraudsters that contact you indirectly:

- Fraudsters are increasingly trying to copy our communications to try and get you to move money or reveal security codes – *we will never ask you to do this via a communication.*
    - Look out for any unusual ways of being contacted – even in the current situation, we will try and stick to our standard practices for contacting you.

3 Unauthorised fraud payments:

If you are a Debit Card holder, please regularly check your statements to see if there are any strange payments. Our Card Service provider will be able to investigate any suspicious payments that you do not remember authorising. If you spot one, please call your Relationship Manager/Director.

4 Authorised fraud payments (APP)

Authorised push payments are when a fraudster has hacked either your email or one of your vendors / suppliers.

4.1 Impersonating a vendor, supplier or third party

They will send what looks like a normal invoice and follow up with an email asking you to change the account into which you normally pay. *Before doing anything, contact the person sending the invoice directly.*

- Do not change your accounts until you have confirmed with the vendor.
- Use a different way of contacting them – if they email you, call the vendor's land line or mobile, and vice versa.
- Make sure you speak to someone you recognise. They will appreciate you having taken the time to inform them

4.2 Impersonating the Bank, an organisation or the Police

Some fraudsters will try and create a sense of urgency – and will pretend to be a bank you hold an account at or even the local police. This should be a warning to you that you should pause. *A genuine bank, organisation or police officer will never ask you to transfer money, take out money, be involved in an operation to catch fraudsters, or divert your payments or change bank accounts*.

- If this ever happens, take the name of the person calling – ask for their employee ID and if police their identity numbers, a contact number and email address, and say you will call them back.
- This buys you time to contact your Relationship Manager/Director and get them to contact the organisation you've been contacted by.

4.3 Impersonating someone from your company

Some fraudsters will pretend to be someone in authority in your company and try and urgently get you to make a payment by sending you an email with payment details. *A genuine senior executive will never ask you to do this over non-work email, without talking to you directly, and will rarely go outside of your established processes.*

- If this happens, try and get hold of the person asking for the payment to be made and either talk to them face to face, or by phone, as long as you are sure you recognise their voice.
- Escalate your concerns to your line manager/supervisor or to the legal department.
- If you are still unsure as you make the payment, voice your concerns to your EAB Relationship Manager/Director, who can look at it from the Bank's side. We are here to support you.

5 Protecting your personal data:

Below are some tips that you may want to consider:

5.1 Protecting your email:

If you have a web email (like yahoo, Gmail or Hotmail), you can set up something called 2 factor authentication by downloading an authenticator app. Your web email provider will help you set this up.

Set up alerts if anyone tries to log onto your email. Your email may have the ability to let you know if someone has tried to log in – this may be you on a different device, but it is a reassuring feature.

Change your password regularly, ideally every few months. If anyone has got access to your account, you will be able to block them out just by changing passwords.

6 Common Coronavirus Scams

We hope this helps you fight crime in these uncertain times, Also please see some of the common coronavirus scams that have been uncovered in recent days:

- GOV.UK Coronavirus Alert – Fines: text messages from an official address saying you have left your residence more than 3 times and a fine has been added to your account (with a link). The fake link asks you to pay the fine by giving your financial and personal details. Sometimes, these appear in the chain of texts alongside previous genuine messages. – *Do not click on any links in the text or email.*
    - Instead, go to the official Gov.uk site and sign-in using your normal Government Gateway address. If you don't use the Government gateway, they will not send you a text message and ask for money.
- Fake online resources – such as a Coronavirus Map. By clicking on your area, you may download a virus
    - Instead, go to trusted resources such as WHO, or an online newspaper that you are already subscribed to
- Refund scams – people offering face holiday refunds for trips you have had to cancel.
    - Instead, use the contact details on the original email confirming your flight/holiday, or get in touch using the company's website
    - Beware when going to a website that it is not a fake – look for the https at the end of the first part of the URL, or use the Google approved site, usually shown on the right hand side of the screen.
- Counterfeit goods – such as sanitiser, face masks, testing kits either sold online or at your door. These products can be fake or even dangerous
    - Instead, speak to your trusted pharmacist or a site you have previously used, or purchase from supermarkets.

- Telephone scams – cold calls from people you are not expecting, claiming to be your utility provider or mortgage lender. If it feels wrong, it probably is.
    - Instead, hang up and go online and call using a trusted number, which may be on a paper bill.
- Donation Scams – There have been several reports of thieves extorting money claiming to be collecting donations for Personal Protective Equipment or to produce a vaccine
    - Instead, go to a trusted source or link (from your online newspaper) and donate that way.
- Fake investment firms – these companies may offer you extremely good returns for placing money with them. If the return seems very promising, it is probably a scam
    - Instead, contact your trusted financial advisors to investigate opportunities, and go to your Relationship Manager/Director to see what opportunities are available.