SECURE BANKING BEST PRACTICES

Best practices against fraud

When transferring funds make sure you are fully aware of where the request originates from. Do not commit to any transactions if you have any doubts.

- Bebawa will never ask you to give your password or one-time-passwords (even if they claim to be bank employees).
- Make sure you only confirm transactions and/or login attempts in the BEBAWA online banking application, that were initiated by you.
- Use Multi Factor Authentication where possible (MFA – a combination of multiple authentication techniques. E.g., password and one-time-password).
- Always use safe a connection. Avoid using public unprotected Wi-Fi. If there is no other choice – add a layer of protection by connecting via VPN prior to connecting to any other environment.
- Make sure you are browsing in a secure manner. The address should start with HTTPS – this way you can be sure the internet connection is secure and encrypted.

INTERNET BANK FRAUD

Mechanics

- You receive an urgent notification from your bank via a phone call, e-mail, or SMS seemingly indicating some sort of error or misunderstanding.
    - An e-mail or SMS directs you to click on a link to a site that looks like your banking login screen.
    - If this is a call, you are asked to provide user ID, PIN codes or card numbers or any other similar log-in information.
- Once the requested information is provided – fraudsters take over. They will use your log-in information to connect to your Internet Banking account and perform unsolicited transactions.

Tips for users

- Your password and one-time-passwords are secret, they should only be known and used by you. No one from Bebawa will ever need or ask for this information from you.
- Do not click on links in SMS or email, it's better to open the bank log-in screen in a separate browser window, and log-in via usual means. Any urgent or relevant information will also be posted in your user account.

INVOICING

Mechanics

- You receive a false invoice for a service provided. These are especially prevalent when working in accounting or financial areas. Alternatively, this may be a message of change of an account number with service provider, stating that from now on all the payments should be sent to a new account instead.

- Fake information may even be disguised under real life service provider name and would usually indicate the amount of money that is in line with previously processed payments.
- Once such payment(s) are executed, it is nearly impossible to trace and/or get a refund.

Tips for users

- If you have a doubt when the invoice is received, a double check should be initiated with the representative of the service provider. This is best done via a confirmed phone number (not the phone number you get in the email) or in person.
- Any time an invoice has a new/previously unseen account number – check with service provider representative for confirmation and reason.

FAKE SENIOR MANAGEMENT

Mechanics

- You receive an email from fake upper management member (usually C level), demanding for a money transfer bypassing usual verification process. In addition to that – transfer is done to an anonymous account. Message usually bears a sense of urgency and is very vague in it's reasoning.

Tips for users

- Have a secondary verification process for non-standard financial transactions. This may be as simple as contacting the person you perceive is sending the message, but via other means, like phone or SMS, and asking to verify the transaction.
- Such bank transfer requests may be reported to a banking institution for them to keep track of transaction.

PHISHING AND SPEAR PHISHING

Mechanics

- An e-mail stating that your bank account is compromised or that there is additional training you need to pass or a similar message requiring you to click on included link. Clicking on the link would open an exact copy of genuine (expected) website.
- By entering credentials, you send a copy of them to the scammer, who in turn can connect to the actual platform under your name.

Tips for users

- Make sure you operate using a secure connection (use VPN if applicable).
- Make sure that sender's email address is genuine - click reply and in the "to:" field you will see real sender's address. If this is not what you would expect – report the scam attempt.
- Never give into the perceived sense of urgency in the email. If unsure – connect to banking platform manually to verify information in the email.
- Report the phishing attempt to your IT and your colleagues. If the attempt was disguised as a bank or any other institution – inform them about the attempt so they can take preventive measures and can communicate to their clients accordingly.

- Never approve an operation if you are not sure you initiated it.

E-MAIL ATTACHMENTS

What are they?

- The email you receive contains an attachment. Message itself may be anything from fake invoice to something akin to “see this funny picture”.
- After opening the attachment, the file executes malicious code on your computer.
- The executable code can be anything from secretly logging information in the background, using resources of your computer, or even taking it over and encrypting the data and demanding a ransom afterwards.

Tips for users

- Always check if senders email address is genuine by pressing reply and checking email address in “TO:” field.
- Make sure you operate using a secure connection (use VPN if applicable).
- If you feel that file/link sent is confusing or not what you expected – close it.
- Report the phishing attempt to your IT and your colleagues. If the attempt was disguised as a bank or any other institution – inform them about the attempt so they can take preventive measures and can communicate to their clients accordingly.
- Never approve an operation if you are not sure you initiated it.