Bank Pocztowy

online banking fraud alert

Online banking is a convenient and secure way of using banking products. When making online transactions, you should, however, bear in mind potential risks and observe basic security rules.

WHEN CAN I SUSPECT AN ATTEMPTED DIGITAL ATTACK?

! When you receive a text message which purports to have been sent by the Bank and which includes:

- a notice of change in your personal data (e.g. your phone number)
- an SMS code to authorise an online banking transaction, **while you did not place any instruction to make the change or transaction referred to in the text message**.

! When you notice in the online banking service that it was last successfully signed into when **you are positive you were not using the service**.

! When you are prompted by your web browser to install a new certificate or the online banking website looks or operates differently than usual, including requesting an SMS code, your personal identification number, etc.

HOW SHOULD I RESPOND?

Immediately contact the Bank to notify it of the suspicious activity you have noticed. You can call the Bank Helpline.

Also remember to:

1. **block access to the online banking service** to prevent unauthorised access to your funds.
2. **go through your recent transaction history** and lodge a complaint if you notice any unauthorised transactions.
3. **remove all malware from all your devices** (PC/laptop/smartphone), preferably with the assistance of a specialist IT service. Using generally available antivirus software may not be sufficient.
4. **remove your online banking credentials** from your web browsers if you have enabled a password saving functionality.
5. **change your passwords and/or sign-in methods** on your other devices if you use linked services (e.g. Gmail) which you automatically sign into on a smartphone or in a web browser.

SOURCES OF MALWARE INFECTION

Malware is usually downloaded/installed as a result of the victim's inattention or ignorance or the hacker disguising it as trusted data or software. There are many ways to infect your devices with malware. Beware in particular of: **messages you receive at your private or business email address which:**

- are written unidiomatically and/or appear to have been machine translated
- promise you a financial gain, e.g. through purchase of gold at a reduced price
- contain attached documents (doc, xls, pdf), archives (rar, zip), or images (jpg, png, bmp, gif).

Never open any attachments from unknown or suspicious senders!

mobile apps which:

- are installed from websites other than official ones (such as GooglePlay or AppStore)
- are installed from websites which fake antivirus software messages notifying you of a "threat" and an option to scan your device "for free".

using weak sign-in credentials, e.g.:

- identical passwords for different websites
- passwords that you have not changed for years and/or that are easy to guess, especially for such services as Gmail, which tends to store a lot of sign-in credentials and which you are automatically signed into on your smartphone or in your web browser.

Regardless of your vulnerability or the infection method applied, malware may be capable of:

- **recording the keys struck on your device keyboard and retrieving such records**
- **taking screenshots on your device and sending them to unauthorised recipients**
- **recording your web browsing history and data your enter on the websites you visit**
- **signalling when your device is online and can be actively used**
- **intercepting incoming text messages**
- **replace an account number you enter in the online banking service with the account number of a third party without changing the value displayed on your screen.**