



Scams and other cyber security risks are on the rise, and one must be cautious and aware on how to identify them. For this reason, it is very important that one stops, looks and thinks before proceeding. Below, one can find some tips on how to be more secure while surfing the internet or using portable devices.



What is phishing?



GDPR Information



Tips for Safer Banking

What is phishing?

Phishing is a social engineering tactic where scammers seek to convince you to hand over your personal details often via malicious links or attachments, usually by email.

Common traits of phishing:


- ⚠️ Asking for personal information
- ⚠️ Suspicious attachments
- ⚠️ A sense of urgency -
- ⚠️ Too good to be true

Avoid phishing by:

- ✓ Checking sender address
- ✓ Hover over any links and check if they are related to the company you are dealing with
- ✓ Verify with sender via a different channel such as phone

Have you received a suspicious email or SMS?

If you received a suspicious email, SMS or phone call claiming to be from MeDirect:

- ⊖ Do not respond to the email or SMS
 - ⊖ Do not open any attachments or click on the URL links contained in the email
-  Call us in 02 518 00 00. The information you provide will be used to help reduce financial fraud.

Tips for safer banking



Update Software

Always update your operating system and applications when the vendors release any fixes or enhancements. Also, only use applications available on your device's official store

Install an anti-virus software

Virus protection software is critical to keeping your personal computer and your online banking safe. Install and regularly update anti-virus and firewall protection on your computer. Scan your computer often.

Be cautious with downloads

Do not download software from unknown or untrusted websites unless you are sure they are safe.

Avoid Public Wi-Fi

Be cautious when using public WIFI. Do not do browse to any sensitive websites such as banking over a public WIFI, unless you are sure it is a secure

Never Reveal Personal Information

MeDirect will never ask you for password or pin. Do not divulge any details of your password to anyone. When possible, always use multi factor authentication.

Backup your device

Make sure your personal computer is backed up. There are numerous cloud options available. If your device is lost or stolen, you'll be able to recover your data

Lock your device

Make sure that your device has a secure password and never leave the device unlocked when unattended. Use biometrics like fingerprint and faceID when available.

GDPR Information



What does GDPR imply?

The General Data Protection Regulation (GDPR) is a set of rules to ensure a better protection of European citizens' data. It is a revision of European legislation from 1995, the Data Protection Directive. The GDPR's goal is twofold: on the one hand it aims to safeguard European citizens' privacy, on the other hand it wants to give citizens more rights as to what happens with their personal data. GDPR came into force on 25 May 2018.

Protection of your personal data

MeDirect ensures that all personal data is securely stored. To protect your personal details against access by unauthorised persons or loss, we have implemented the necessary technology and ensure it is kept up to date.

In the event that third parties offer a service to MeDirect, a contractual agreement ensures third-parties implement the correct security procedures to safeguard your personal data such as working with encrypted information. The transfer of personal data to third parties will only be for purposes laid down in our agreements with clients and/or our term and conditions.

What is included in our privacy policy?

In adherence with GDPR legislation, we amended our [privacy policy](#). This privacy policy defines which information we collect of every person, why we collect this information and with which parties this information is shared. The privacy policy also defines your rights and specifies MeDirect contact if you have questions relating to the security of personal data.

What measures did MeDirect take to be in line with this legislation?

Various initiatives were implemented to protect our clients and employees, such as:

- An amendment of our privacy policy.
- Giving privacy training to all our employees.
- Amendment of our general terms and conditions and cookie policy.
- Training to our employees concerning HR requests.
- A review of how we ask whether someone wants to be informed of our commercial offers or newsletters.
- Amendment of internal policies to ensure they are in line with GDPR legislation.