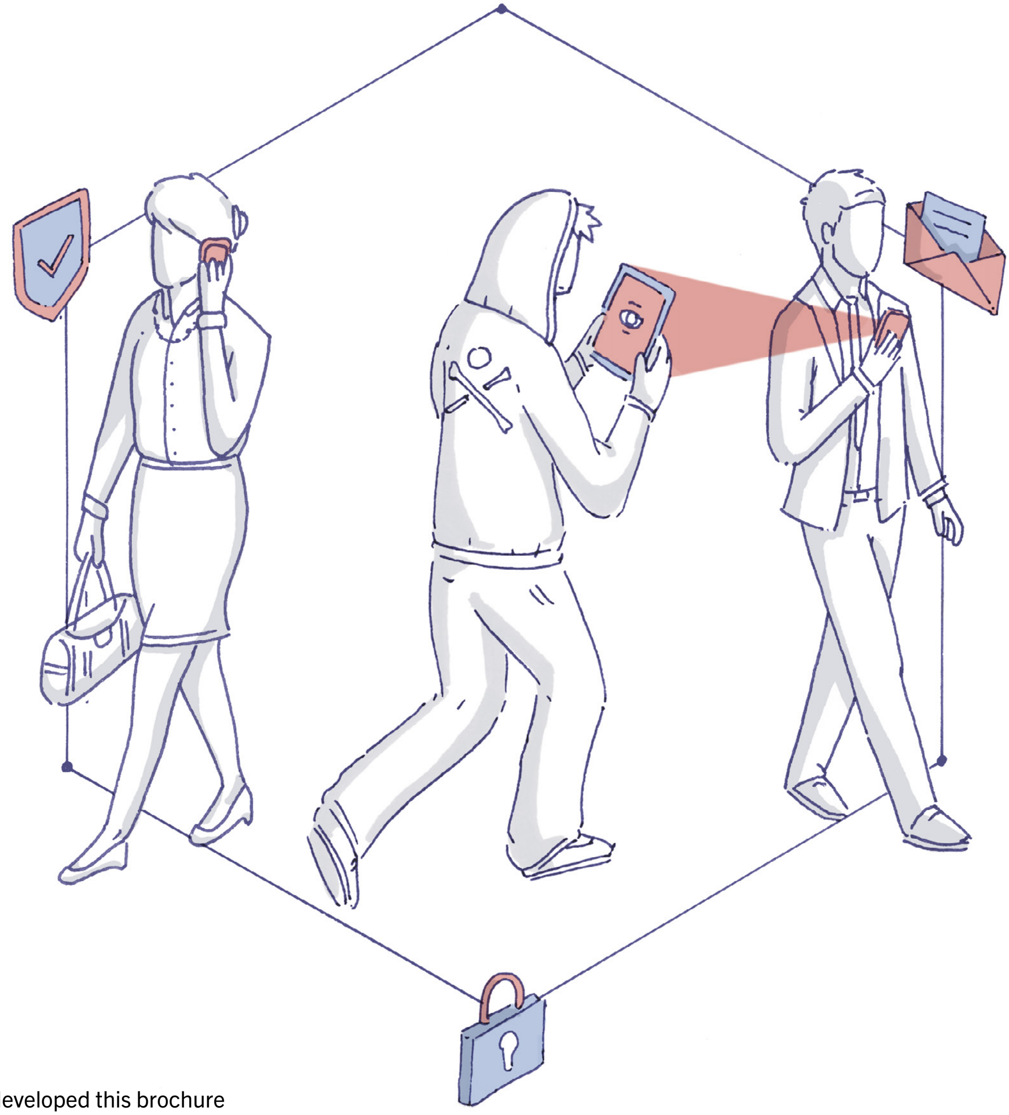
PICTET
1805

JANUARY 2020

CYBERSECURITY

PROTECTING AGAINST DIGITAL RISKS



We have developed this brochure to give you important information about the risks related to cybersecurity and how you can protect yourself against an attack.

PERSONAL DATA THEFT IS ON THE RISE

Personal data has become a commodity. We use it to log into free platforms like social networks, messaging systems and public Wi-Fi networks. But most of the time, we aren't fully aware of the security systems these platforms have in place. The organisations that collect our data may use it for commercial purposes – legally or otherwise.

We should therefore be extremely careful when shar-ing our personal data. This is especially important given the rise in data breaches where user behaviour is not always a factor. Even large IT companies are vulnerable: the Cambridge Analytica scandal at Facebook affected 87 million users, and the 2018 data leak at Google affected 52 million users.

At Pictet, our primary goal is to look after our clients' long-term interests. That includes protecting the integrity of your personal data and making sure you are aware of potential risks. We have therefore put together this brochure to give you useful tips on how to protect yourself against cyberattacks.

Sensitive information, including a person's identity, precise location and passwords, can easily fall into the hands of criminals. They can then use this information to hack into your accounts or hijack your device. By taking a few simple measures, you can reduce your risk considerably. Pages 4 and 5 of this brochure give advice on making your online accounts more secure, and page 6 tells you what to do if your data is stolen. We suggest you read this brochure carefully and keep a copy close at hand.

January 2020

HOW CYBERCRIMINALS OPERATE

Criminals can collect your personal data without your knowledge and then use it to log into your accounts illegally or hold your computer to ransom by encrypting your files.

Cybercriminals have come up with a number of clever ways to steal your data. These include piecing together bits of information you have inadvertently made public in order to guess your passwords, hack into your devices or steal your identity.

They may also send messages that play on your fears ("a virus has been detected on your computer"), evoke empathy ("help a friend in trouble"), create a sense of urgency ("immediate reply required") or promise attractive gains ("don't miss this one-time opportunity").

Here are some examples of the tricks cybercriminals use:

1. DIRECTING YOU TO FAKE WEBSITES

You receive an email – apparently from someone you know – asking you to click on a link to a (fake) Pictet website, for example. The website looks just like the original, except the URL address is slightly different: picttet.com, plctet.com or pic-tet.com. Once you're on the fake website, the cybercriminal can easily record any information you enter.

2. HIJACKING YOUR COMPUTER

You receive an email containing an attachment from someone whose identity has been stolen. Once you open the attachment, a ransomware program takes over your computer and displays a message demanding you pay a ransom (typically via a cryptocurrency) to regain use of your system.

3. PRETENDING TO BE THE CEO

You receive a message – ostensibly from a CEO or another senior manager – asking you to provide confidential information in response to an urgent situation (such as a cross-border acquisition or a tax audit).

TIPS FOR KEEPING YOUR DATA SAFE

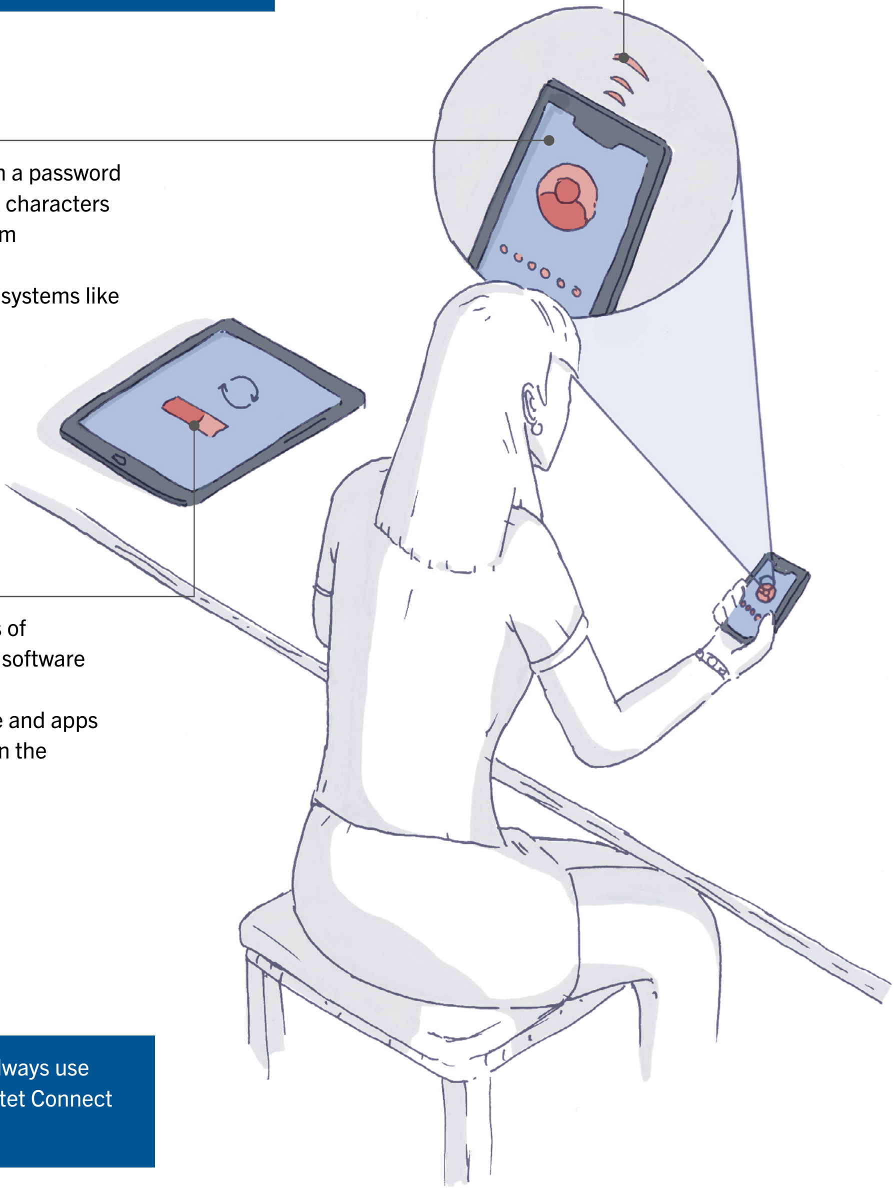
Here are some simple steps you can take to reduce the likelihood of a cyberattack.

Enable features that let you remotely wipe your devices if they are lost or stolen

Don’t keep confidential information (like passwords and bank account details) in your email inbox

Protect your devices with a password containing more than six characters or with a biometric system

Don’t disable protection systems like PIN codes



Allow automatic updates of applications and system software

Don’t download software and apps from a website other than the developer’s

When contacting us at Pictet, always use one of our secure channels (Pictet Connect or our mobile apps).

Double-check websites’ URL addresses

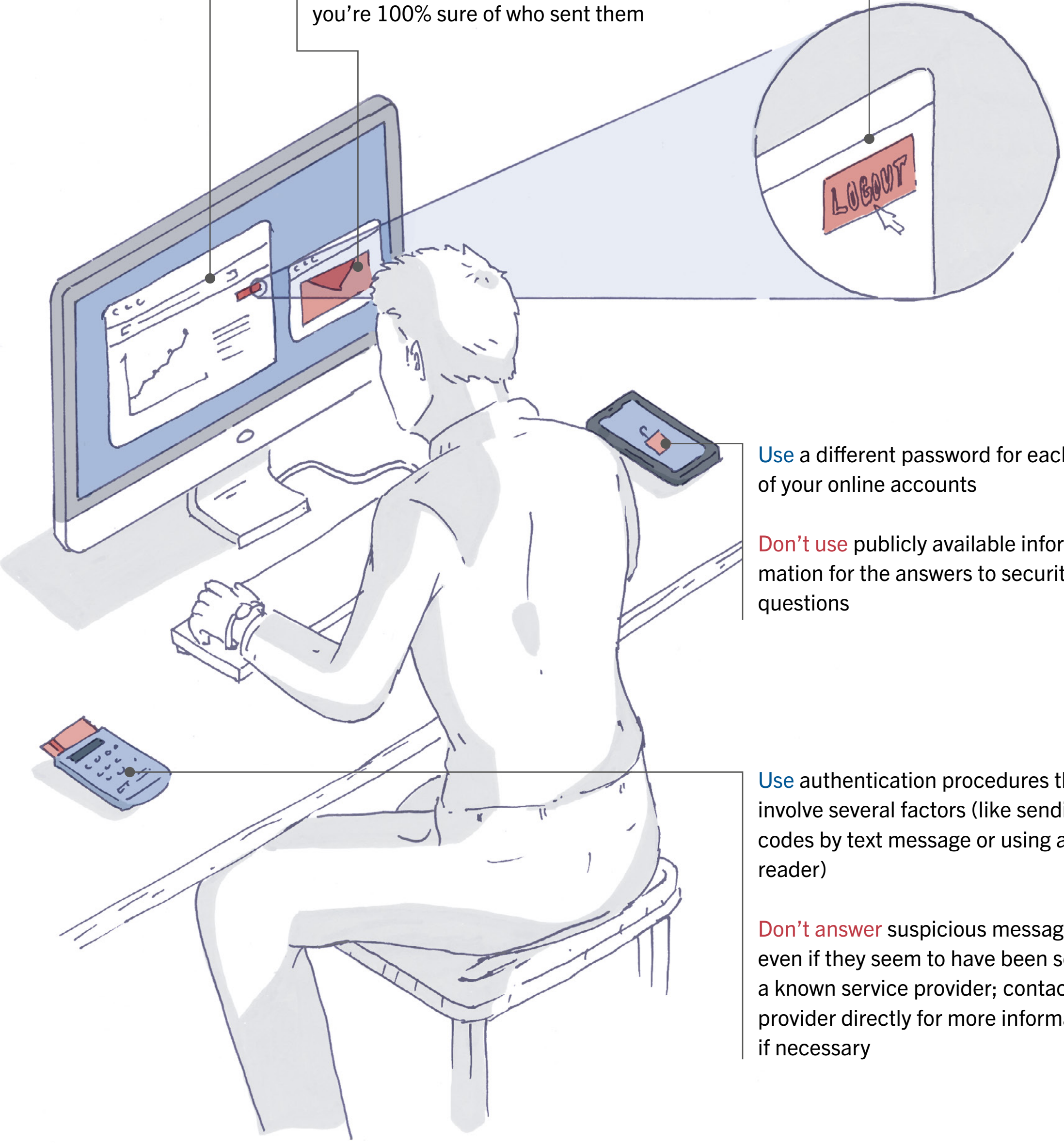
Don’t enter sensitive information on an unencrypted website, especially when using a public network

Use a healthy dose of scepticism when you receive unsolicited emails

Don’t open attachments unless you’re 100% sure of who sent them

Close all sessions by logging out properly

Don’t leave a session open on an unattended computer or device



Use a different password for each of your online accounts

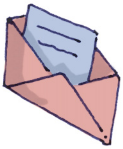
Don’t use publicly available information for the answers to security questions

Use authentication procedures that involve several factors (like sending codes by text message or using a card reader)

Don’t answer suspicious messages, even if they seem to have been sent by a known service provider; contact the provider directly for more information if necessary

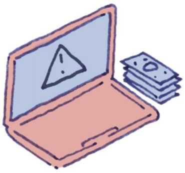
WHAT TO DO IF YOUR DATA IS STOLEN

If you believe you have been the victim of a cyberattack, take the following measures immediately.



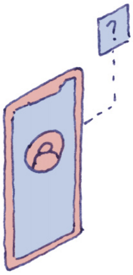
IF YOUR EMAIL ACCOUNT HAS BEEN HACKED

- Follow the service provider's instructions for recovering access and change your password immediately (for this account and any other accounts that use the same password)
- Tell your contacts that your account has been hacked and that they should not trust any messages from that account for the time being
- Identify what confidential information the hacker might have accessed through your email account (such as bank account information or other sensitive data) and contact anyone who might be affected
- If your email account has been hacked, check whether the hacker has set up an automatic reply or changed any other settings



IF YOUR COMPUTER HAS BEEN HIJACKED BY RANSOMWARE

- Don't pay the ransom
- Contact an IT security expert immediately



IF YOU ACCIDENTALLY PROVIDED SENSITIVE INFORMATION TO A POSSIBLE CYBERCRIMINAL BY TELEPHONE

- Change all passwords that could be at risk
- Tell everyone who might be affected (colleagues, friends, etc.)
- Block the person's phone number and don't respond to any further contact attempts

HOW TO SPOT MALICIOUS EMAILS

There is no foolproof method for identifying malicious messages, but some signals should be considered red flags.

It is important to be wary of messages:

- displaying an unknown or unusual email address, especially if it looks similar to an address already in your contact list;
- utilising suspicious wording, a threatening tone or a message pushing you to act right away;
- making vague promises or offering an opportunity that sounds too good to be true;
- encouraging you to open an attachment or click on a link to view the full content;
- not clearly stating who the intended recipient is or coming from an email address that the (supposed) sender has never used before.

Of course, not all emails with one of the above red flags are malicious. But these are certainly signs that should prompt you to proceed with caution.

Legal information

This document is not aimed at or intended for distribution to or use by any person who is a citizen or resident of, or domiciled in, or an entity that is registered in, a country or other jurisdiction where such distribution,publication, availability or use would be contrary to law or regulation. The information and material are provided for information purposes only and are not to be used or considered to be an offer or solicitation to buy, sell or subscribe to any securities or other financial instruments. Furthermore, the information appearing in this document is subject to change without prior notice.

Pictet
Pictet is a partnership of seven owner-managers. Its principles of succession and transmission of ownership have remained unchanged since foundation in 1805. It offers only wealth management, asset management and related asset services. The Group does not engage in investment banking, nor does it extend commercial loans. With CHF 544 billion in assets under management at 30 June 2019, Pictet is today one of the leading Europe-based independent wealth and asset managers.

Founded and headquartered in Geneva, Switzerland, Pictet today employs more than 4,300 people. It has 27 offices in: Amsterdam, Barcelona, Basel, Brussels, Dubai, Frankfurt, Geneva, Hong Kong, Lausanne, London, Luxembourg, Madrid, Milan, Montreal, Munich, Nassau, Osaka, Paris, Rome, Singapore, Stuttgart, Taipei, Tel Aviv, Tokyo, Turin, Verona and Zurich.

Produced by
Large Network

www.group.pictet