ISABEL
E-SECURITY

MONITOR AND PROTECT YOUR ONLINE TRANSACTIONS.

isabel group

SECURE ONLINE BANKING WITH ISABEL 6.

Isabel Group offers innovative security.

Computer crime is a real threat, and the techniques and methods are constantly evolving. Isabel Security Services focuses on innovative developments to stay one step ahead of the fraudsters and limit the risks to a minimum.

Isabel 6 guarantees secure financial transactions. It is a multi-bank solution that gives professionals access to all their accounts with different banks on a single screen:

- 30,000 companies, self-employed, organisations and governments use Isabel 6 every day.
- In 2015 Isabel 6 was used to transfer more than 2,600 billion euros.
- The Isabel 6 smartcard is accredited by the government for the secure access to applications such as Tax-on-web.

Opening an attachment or reading an email in preview is all it takes to activate a virus. Unfortunately, there are many ways to break into financial transactions. Make no mistake: hackers also target small companies. Multinational companies often have a professionally equipped IT department to ensure their security, but resources are limited for small to medium sized businesses. Fortunately, you do not have to be an expert to take preventive action: Isabel Group is at your service as your expert.

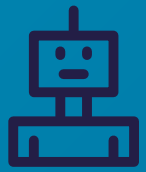
Trust our specialists and tools to protect your banking.

COMPUTER CRIME:
WHAT ARE THE DANGERS?

The intrusion can occur before or during a financial transaction and a range of techniques can be used. Criminals often use a different identity to mislead your computer or the person using it.

Phishing

A criminal can pretend to be a trustworthy person sending you an email requesting sensitive financial information or even your username and password.



BotNets

A BotNet is a network of computers controlled by cybercriminals. Your computer can be included in this network without your knowledge.

False billing

You are sent or emailed a fake invoice that looks as though it was sent by one of your suppliers, but is showing a different account number.

Malicious software

Criminals can use viruses and other malware to access your computer and system remotely.

COMPUTER CRIME:
WHAT ARE THE DANGERS?

Mule Accounts

People are recruited online to transfer stolen money on behalf of criminals. Often these money mules are not even aware that they are involved in illegal practices.

Stolen identity

Criminals take on someone else's identity online to steal financial information and even apply for loans.

CEO fraud

The attacker sends a confidential email to a Finance member of staff in the name of the CEO asking the employee to transfer funds. The criminals often simply find the information they need on the company's website or social media channels.

Man in the Middle

A third party intercepts your communication with the bank by taking over your browser. It will seem as though you are signing transactions you created yourself, but in reality you will be authorising false payments set up by hackers.

MALWARE: WHERE IS THE WEAKEST LINK?

By secretly installing malware on your computer, criminals can compromise your online banking. This can cost you a lot of money, so the security of your computer is extremely important.

How is malware used?

- A virus is a small programme that disrupts the operation of your computer.
- Spyware is software that collects sensitive data such as passwords and account numbers, which are then sold on the black market. A keylogger can record all the keys struck on your keyboard, for example.
- Ransomware is covertly installed on your computer and demands that you pay a ransom to unlock your device again.

MALWARE: WHERE IS THE WEAKEST LINK?

Malware can steal your personal information, give others access to your system and even make your computer unusable. Be vigilant, because prevention is better than cure.

Testimony

"I received an invoice from a supplier by email and when I opened the attachment, it seemed to be a blank file. Strange. I checked the email again and then I noticed that the actual sender was not my supplier. I deleted the message, but I later found out that the malware had already spread on my computer."

FRAUD:
DO NOT BE MANIPULATED.

Although cyber-attacks are becoming increasingly inventive in a technical sense, many fraudsters will not hesitate to contact you in person to mislead you.

Social Engineering

Someone pretends to be a person you know and trust and asks you to pay a large sum of money urgently. This fraudster gains information about your company and your colleagues on social media and other channels to try and convince you of his false identity.

Testimony

"I received a phone call from a 'colleague' who was away on business. He asked if I could quickly transfer a substantial sum of money to a foreign account to conclude a contract with a new partner. The deal was not yet sealed, so I had to keep the transaction confidential. Those were also the exact words of the confirmation email that was sent to me from a private address. I was also called a few times and asked to pay as soon as possible."

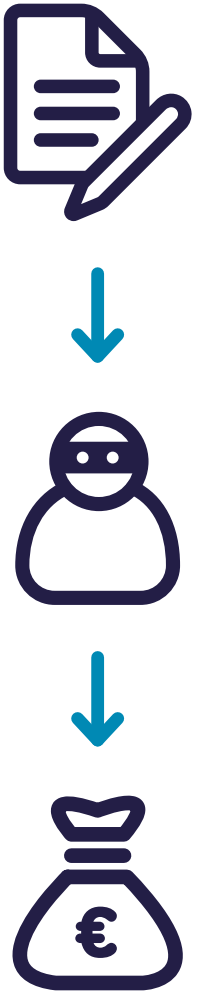
FRAUD:
DO NOT BE MANIPULATED.

Your banks and Isabel Group will never ask you to provide your PIN or password. That information is strictly confidential. If you are unsure of an unexpected request by phone or e-mail, talk to a colleague or your boss. Also never tell strangers who is responsible for your company's payments.

Forgery

When criminals 'break into' your transactions, you will unintentionally transfer money to their **mule accounts**.

- They intercept a bill and change the account number without you noticing.
- An intruder infiltrates your accounting software and edits the account numbers there at the source.
- If fraudsters can get to your payment files, they can also add their mule accounts.



PREVENTION: LIMIT THE RISKS.

You are not a defenceless victim. Fortunately, there are easy ways of stopping fraudsters. Of course vigilance is the shared responsibility of your accounting, IT, management...

What can you and your colleagues look out for?

ON A TECHNICAL LEVEL

- Update your operating system and internet browser.
- Use recent versions of antivirus programmes.
- Make sure your firewall is permanently active.
- Only activate macros if necessary.
- Install a site filter and possibly an ad blocker.

PREVENTION:
LIMIT THE RISKS.

What can you and your colleagues look out for?

IN EVERY-DAY USE

Do not just open any email attachments or links.

Do not visit unreliable websites.

Do not use infected USB sticks.

Do not share too much (professional) information on social media.

Look out for strange messages or screens.

Be extra vigilant during holidays.

PREVENTION:
LIMIT THE RISKS.

What can you and your colleagues look out for?

FOR TRANSACTIONS

Restrict access to your accounting software.

Check the sender of the payment request.

Do not immediately meet unexpected requests.

If in doubt, always consult a colleague.

Check your payments twice before signing.

Keep payment files in a safe place.

PREVENTION: INCREASE YOUR SECURITY WITH ISABEL 6.

To help you act proactively and shield your financial transactions from criminals, we developed Isabel 6, a robust tool that complements your current accounting software.

Isabel 6: a better overview, more control

If you have several business accounts or if you are working with two or more banks, you can use Isabel 6 to combine and process all your transactions in one clear environment.

Thanks to Isabel 6, you can also protect yourself with components that significantly improve your user identification:

- Your own personal smart card with PIN
- A direct, secure connection between your computer and card reader
- A reader with keypad (against keyloggers)

PREVENTION:
INCREASE YOUR SECURITY WITH ISABEL 6.

Isabel 6: more possibilities, more security

An extra overview also means extra monitoring. The synchronisation between your accounts and Isabel 6 ensures that all information is transmitted accurately, both internally and to the banks. This reduces the risk of data manipulation.

The smart features of Isabel 6 also allow you to optimise your internal procedures:

- Share verified beneficiaries and keep them in one list.
- Use a detailed payment summary to perform targeted checks.
- Have any suspicious transactions reported by phone.
- Consult your bank(s) to determine the authorisation of every employee with mandates.
  - Who can see which information?
  - Who can create payments?
  - Who can sign for payments?
  - What is the payment limit?

PREVENTION:
INCREASE YOUR SECURITY WITH ISABEL 6.

Isabel 6 MultiSign: even more security

Four eyes see more than two. MultiSign makes it even easier for you to invite a colleague or partner to check and sign important transactions. In order to reduce the risk of errors and fraud even more, it is best to request a personal Isabel 6 card for every signatory.

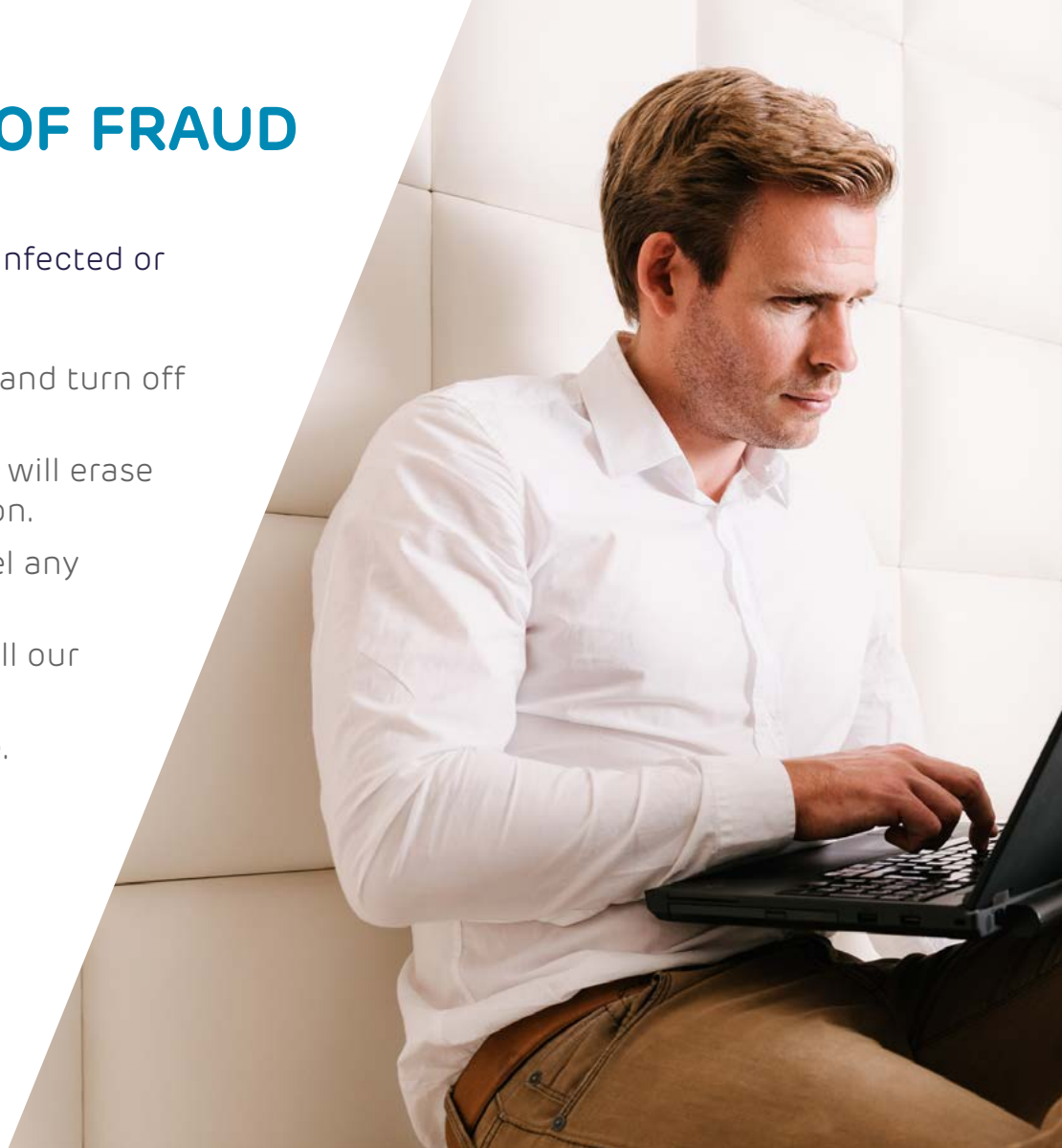
Did you know that you can assign more than two signatories for large payments? Contact your bank to discuss the options.

WHAT TO DO IN CASE OF FRAUD

If you notice that your computer has been infected or hacked, follow these recommendations:

1. Remove your computer's network cable and turn off the computer's Wi-Fi.
2. Do not switch off your computer, as this will erase data that can be used in the investigation.
3. Contact your bank immediately to cancel any fraudulent transactions.
4. As an Isabel 6 customer, you can also call our customer service from 8am to 6pm.
5. Report the incident to the federal police.

Lost or stolen bank card?
Call Card Stop on 070 344 344.



We like to make things easy for you. With 20 years of experience and extensive expertise in secure multi-banking, we offer you tailor-made advice and guidance.

Your requirement

- Protect your computer against malicious software
- Optimise the security of your financial transactions
- Follow the latest updates and developments

Our solution

- Install Isabel 6
- Register to our newsletter

SAFE INTERNETBANKING .BE

CONTACT US
Discuss all your options without obligation on **02 290 55 90**.

You are a professional. So are we.

SECURE ONLINE BANKING WITH ISABEL 6.

Discover our range and all the benefits
on **www.isabel.eu**

isabel group