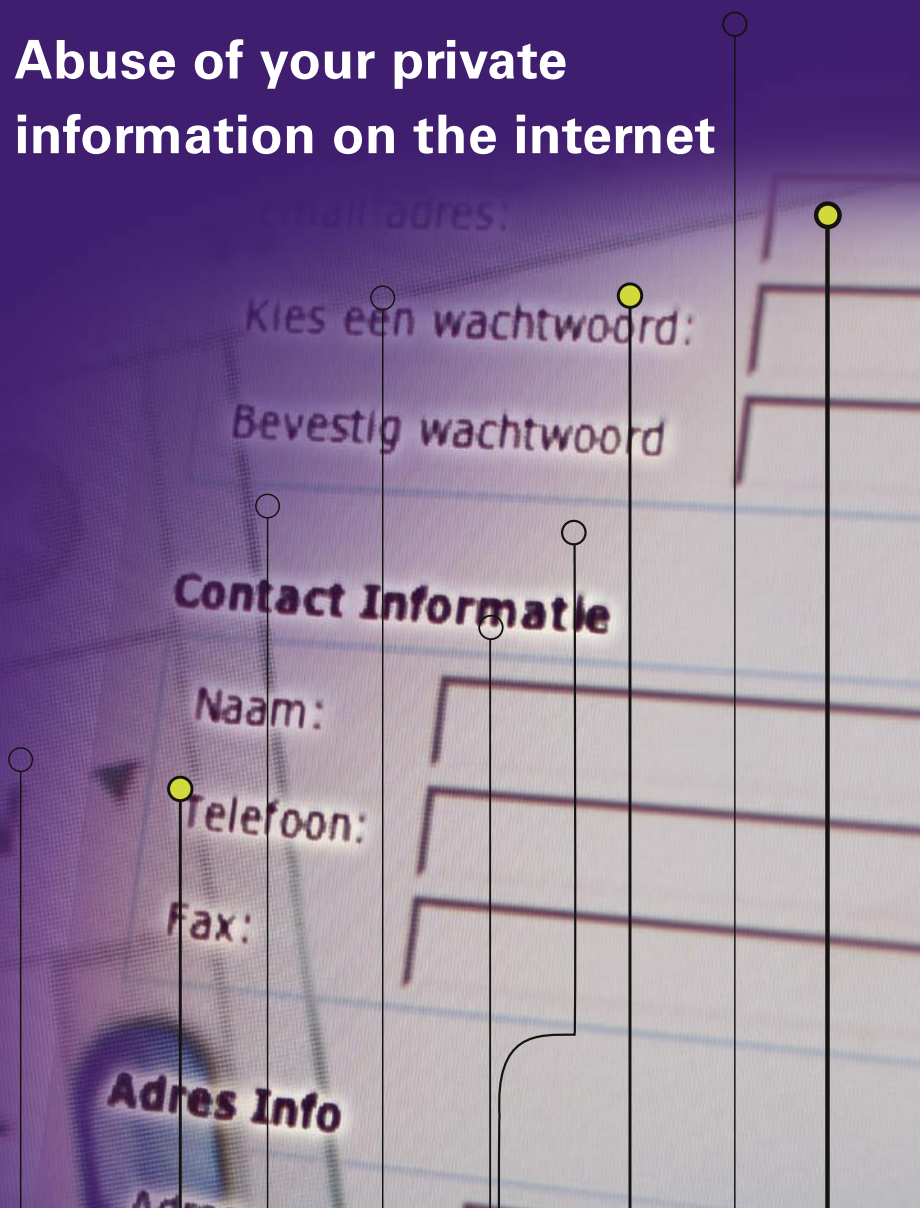


# Phishing

Abuse of your private information on the internet



**Perhaps it has already happened to you: criminals have tried to get your private data on the internet.**

**Unfortunately, this type of criminal activity, which is known as phishing, is on the rise.**

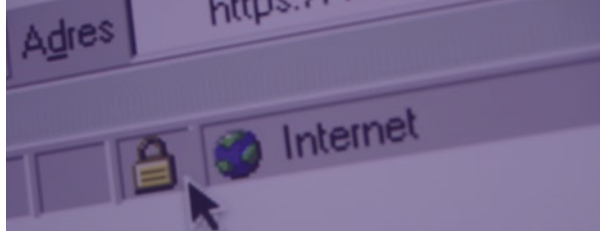
**But what exactly is phishing? How do you recognise a phishing attempt and how can you protect yourself against it? This brochure provides you with brief answers to these questions.**



## What is phishing?

Phishing is a type of deception designed to steal your identity. In phishing scams, criminals try to get you to disclose valuable personal data (like credit card numbers, passwords, account data, or other information) by convincing you to provide it under false pretences.

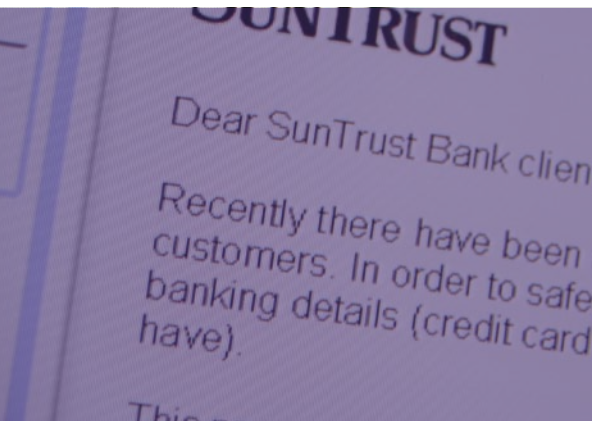
Phishing is on the rise. Criminals have expanded their activities unto the internet and have launched a range of phishing attacks. Even though few people actually fall for phishing tricks, the large number of phishing attempts means a good number of people get hit.



## How does a 'phisher' work?

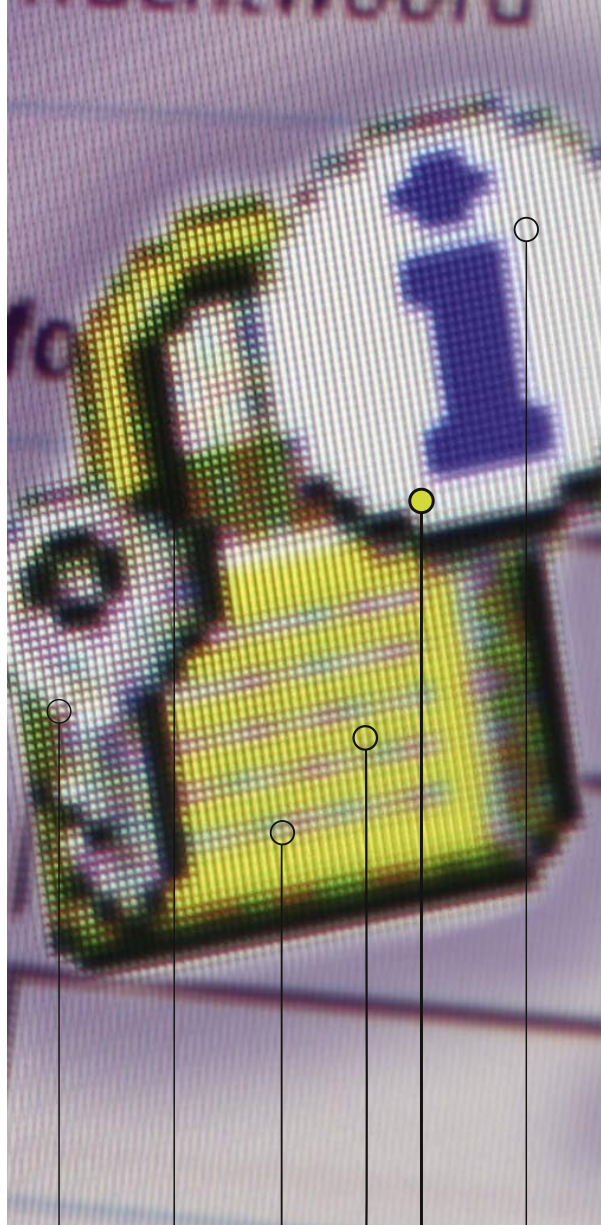
The most common phishing method involves e-mails that claim to be coming from a trusted organisation such as a bank. The e-mail requests you to visit the organisation's site in order to enter your private data. In fact, the website is a fake that looks exactly like the one from the legitimate organisation. Even the internet address in your browser's address bar appears to be the same, though small discrepancies can be noticed upon closer inspection. Sometimes the real website is shown, but you are requested to type in your private data in a pop-up. Data that is entered into it can be immediately used, for example to make purchases.

Phishing e-mails are often sent in bulk in the hope that a small number will be received by actual clients of that organisation. Those who are unaware that the e-mail is part of a scam, may believe the e-mail is legitimate and act upon it.

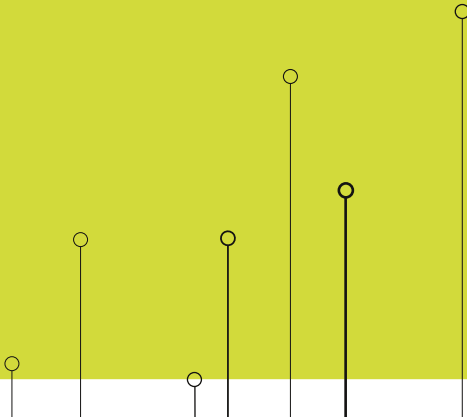


## How do you recognize phishing?

- Phishing e-mails tend **not** to be **personalised**. You are addressed as “Dear client”, “Dear [company name] client” or “Dear user” and sometimes you are not addressed at all.
- Most banks, credit card companies or other legitimate businesses will **never** ask you for your private data, passwords or credit card data **via e-mail**.
- Often, phishing e-mails try to **play on fear** that you will be scammed or that your account will be closed. The e-mail often stresses “urgent reasons” for you to react, such as security breaches or the fact that your account is about to expire.
- The large number of phishing e-mails and their unsolicited nature put them in the **spam** category. If you use a spam filter, it will probably mark the e-mail as spam.



# What can you do?

- If you think you have received an e-mail from a company of which you are a client, but suspect the message is fake, don't click on the link contained in the message. This link could take you to a fake website. Always **go to websites by typing in the internet address in the appropriate bar** in your browser.
  - If you do provide a trusted organisation with private or sensitive data (such as credit card details) make sure you do so through a **secure connection**. If this is the case, the internet address will be preceded by `https://` rather than `http://`. In addition, you will see an icon representing a (closed!) lock in the lower right corner of your browser. Click on that icon for more security-related information, such as whose certificate it is and who issued it. Remember this the next time you check it.
  - Make sure your **browser, operating system and virus scanner are always up to date**, preferably by using their automatic update feature.
  - Install a **spam filter** or subscribe to a spam filter that often is provided by your internet service provider.
  - Regularly **check bank and credit card statements**.
  - **Block** credit cards, bank cards and accounts when you suspect they are being abused.
  - **Alert the party** in whose name the phisher is operating.
  - **Report any actual damage** caused by phishing at your local police station.
- 

**For more information and questions about phishing and other internet-related risks, go to:**

[www.surfopsafe.nl](http://www.surfopsafe.nl) (dutch only)

[www.enisa.eu.int](http://www.enisa.eu.int)

[www.govcert.nl](http://www.govcert.nl)

This brochure is a production of the Netherlands Ministry of Economic Affairs. It is a translation of the Dutch phishing flyer that is made available in English. This brochure can be used in all nations free of rights.

december 2005

GOV<



Ministry of Economic Affairs