



Q & A

What is Card Security and who is behind it?

Card Security is a national prevention initiative that is championing the need for protection against debit and credit card fraud. It is actively involved in systematic campaigns directed at the general public by means of social media, the website [card-security.ch](https://www.card-security.ch) as well as media reports and the information channels of other stakeholders. Preventive work focuses on raising awareness of current scams and identifying guidelines for dealing with debit and credit cards. Specialists from the police and financial institutions can also use the platform to obtain in-depth information on the subject.

The prime mover behind Card Security is the police. The initiative is supported by the Card Security Association, the board of which is composed of representatives of card issuers and the police. It also receives widespread support from the police, card issuers and banks.

Why do we need Card Security?

Crimes with credit cards or debit cards are increasing at an annual rate of 10 to 20 percent. Card Security is the central point of contact of the police for all questions regarding the misuse of debit cards and credit cards. Card Security combines the expertise of various specialists from the police, financial institutions and card issuers. The website [card-security.ch](https://www.card-security.ch) provides cardholders, the police and bank staff with comprehensive information on the latest card offences and all preventative measures.

Card Security is also aimed at specialists in this field. On [card-security.ch](https://www.card-security.ch), police forces and banks can find information on current campaigns and reference information as well as texts on the subject.

"LINDA protects against phishing!" – What does that mean?

The slogan of Card Security's 2026 campaign is "LINDA protects against phishing!" LINDA is a fisherwoman and each letter of her name stands for a phrase that can be used to prevent phishing:

- L** = Links and attachments must be questioned
- I** = Information must be carefully checked
- N** = Neutral greetings are suspect
- D** = Deadlines and urgency are fishy
- A** = Addresses must always be verified

The abbreviation LINDA therefore helps card users remember the most important things to do when dealing with debit and credit cards, and helps to avoid successful cases of phishing.

Who is the target audience for Card Security?

The general public, especially those who have debit cards and credit cards. The platform also provides a large amount of helpful information to specialists in the police and financial institutions.

Have card crimes increased in recent years?

In the past, card crimes were mainly concentrated at payment terminals and ATMs. These so-called "skimming cases" have declined sharply. Nowadays card crime is mostly online. Card offences are increasing at a rate of between 10 to 20 percent per year.

What are the most common card crimes on the Internet?

Most card crimes on the Internet start with phishing. Fraudsters use skilful ruses to trick their victims into disclosing PIN codes, SMS codes, CVC/CVV numbers or passwords. For example, they use fake websites or QR codes, links in emails, phone-calls or text messages (SMS, WhatsApp, Messenger, etc.). The perpetrators later use this data to steal money from their victims.

How are customers supposed to prove they have not fallen for phishing?

That's difficult. Victims often do not even remember receiving a phishing e-mail and disclosing their details. In most cases, quite some time elapses between the acquisition of data and the fraudulent transactions.



Why don't banks take responsibility for fraud cases or show more goodwill?

Liability is governed by the contracts agreed between the bank and its clients. In the event of a dispute, the question of liability must be resolved by a court in each individual case. However, you can be sure that if the client has breached their duty of care, the bank will not accept liability.

Does it make sense to file charges against unknown persons?

Yes it does. As perpetrators move around on the Internet they leave a trail which can be followed. Because of the concealment tactics they employ, it is however difficult to get at the perpetrators. This is why the police stress the importance of reporting these offences. This is the only way for the police to obtain important background data for their investigation and recognise the extent of the threat.

Only when the police (as prosecutors) have the overall picture can they initiate cross-border measures. The new knowledge they gain from reports of cyber fraud also enable them to enhance their preventative efforts.

Because of the perpetrators' methods of operation, it may be difficult to establish where the money went. So-called "money mules" (money launderers) are often used. These operate in countries that pose major challenges for the police, or the fraudsters use anonymous services to cover their tracks.

So is cash safer after all?

Cash is becoming less and less important. Payment by cash is often no longer an option. It is therefore all the more important that cardholders protect themselves as much as possible when using credit or debit cards, and take these few preventative tips to heart. Following these preventative tips allows users to avoid the majority of cases of card fraud.

These tips are summarised on the prevention platform card-security.ch.

What can I do to protect myself from card fraud?

Always remember LINDA and her anti-phishing tips:

L = Links and attachments must be questioned

I = Information must be carefully checked

N = Neutral greetings are suspect

D = Deadlines and urgency are fishy

A = Addresses must always be verified