This is how I protect myself.

» Distrust messages from unknown senders.

» Never click on links, never open attachments.

» Always check the sender’s e-mail address and URL.

» Log in only via official websites (not via links).

» Keep your web browser and operating system up to date.

» Never give out your login and card data.

» Use strong passwords and 2FA.

» Activate a notification service to receive a message when payments are made.

» Check your transactions and payments.

Test your knowledge!

What else can I do?

» Ask your bank or card issuer about the security features of your card.

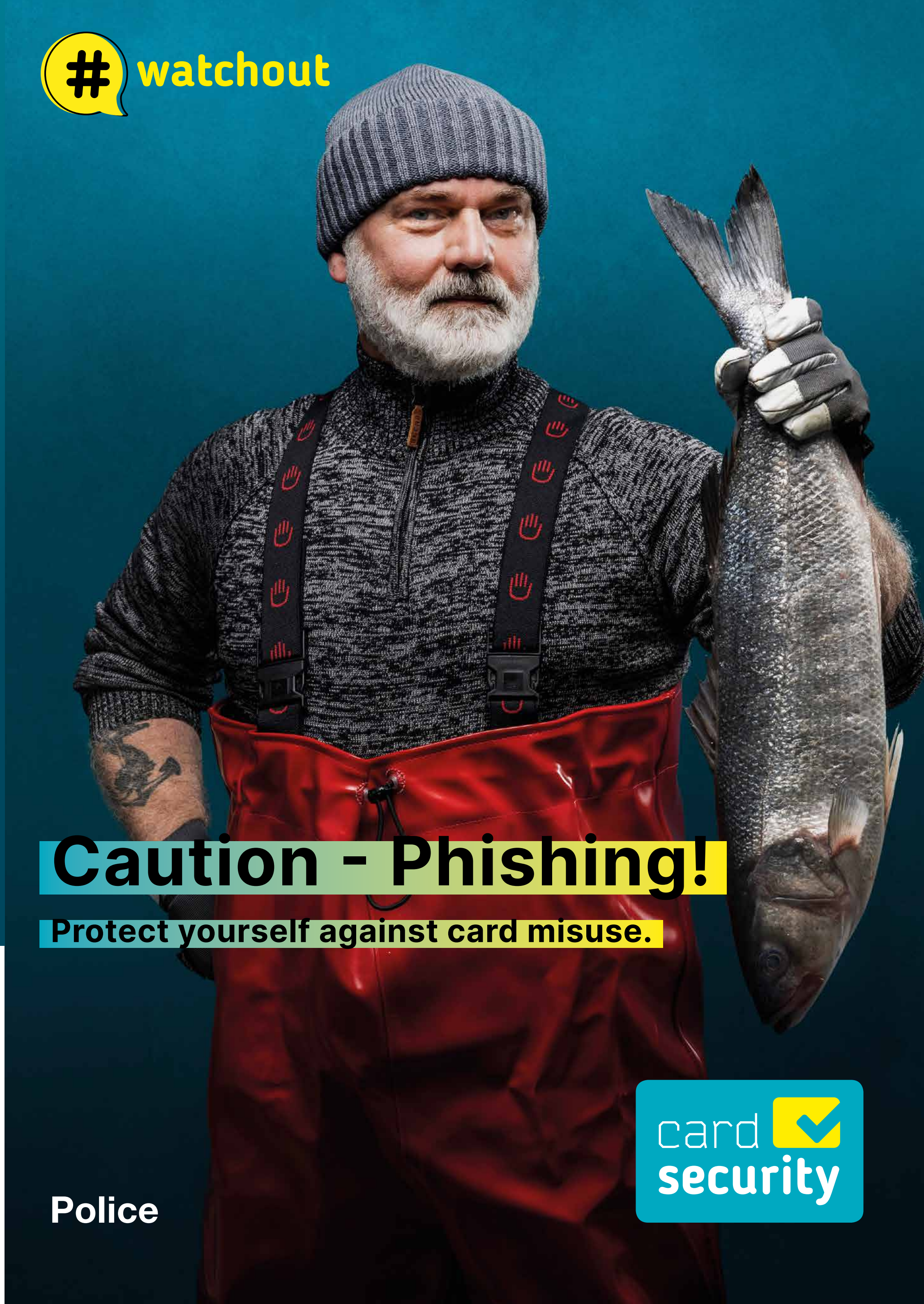
» Activate only those card functions you actually use in everyday life.

» Report every theft to the police.

Learn more about card security at
www.card-security.ch

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali



#watchout

Caution - Phishing!

Protect yourself against card misuse.

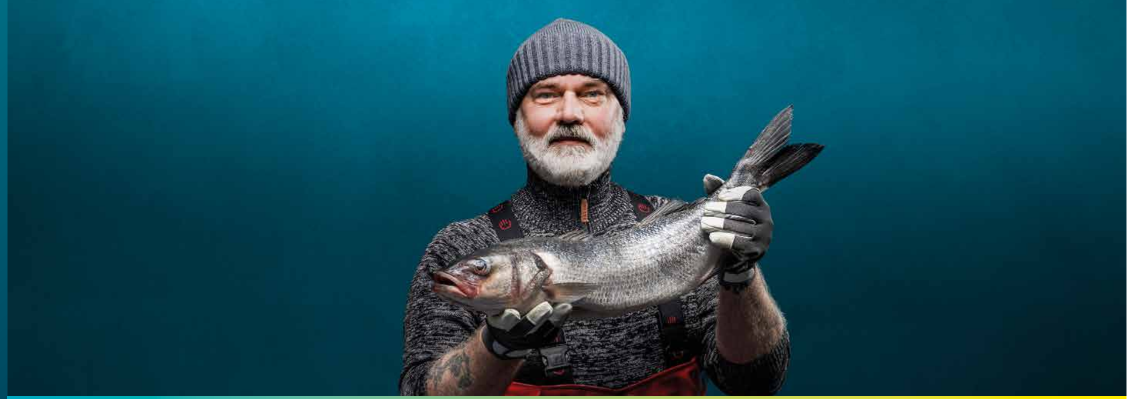
Police

card security

#watchout for these types of SCAMS

Debit and credit cards offer a very secure and popular means of payment; but their widespread use attracts scammers and fraudsters. They try to steal money from their victims using a constant succession of new scams. Most card offences can be prevented if cardholders follow a few basic rules.

Phishing — Pharming — Carding — Scamming



Phishing

Phishing attacks often differ in their presentation and tone. But the basic principle is always the same. The potential victims receive messages via e-mail, mobile phone or social media. These look like messages from a bank, card company or delivery service. The victim is asked to follow the link in the message. Anyone who clicks on the link is taken to a fake page where they are asked to disclose personal information. Anyone who is not careful here can lose a great deal of money.

Pharming

This type of fraud is related to phishing. Users enter a correct web address but fail to notice they have been redirected to a fake page. This is achieved with the help of a virus or a Trojan horse. As with phishing, victims are then asked to enter personal data and card information. Once they have this information, the fraudsters are free to steal money without any problems. The type of fraud is called "pharming" because the fraudsters often operate entire server farms with fake websites in the background.

Carding

In carding, perpetrators use stolen or falsified card information to make online purchases or withdraw money from ATMs. They prefer cards or online shops that provide poor levels of protection. The data were collected illegally beforehand through phishing fraud, data protection violations or skimming, and were sold on carding forums, mostly on the dark net. The victims notice the fraud only after the money has already been stolen. Often months can pass between the time the data were stolen and when the actual fraud is committed.

Scamming

In scamming, fraudsters try to lure their victims with tempting offers. All these propositions are aimed at getting the victims to make advance payments under false pretences. Scamming has many faces: Fraud with false love (Romance Scam), fraud with false promises of money (Investment Scam), fraud with offers of accommodation (Flatmate or Holiday Scam), fraud with the dream job (Employment Scam) or promises of lottery winnings (Lottery Scam).