Checklist

How to spot financial fraud

✓		Core rules:
☐	**Watch out for warning signals**	We all are sometimes a bit careless when it comes to e-mails, messaging or the internet in general. Criminals take advantage of that. Looking out for the warning signals described here can help you spot fraud. Keep in mind: Companies and banks never ask for confidential data like passwords or login details via e-mail, text message or phone.
☐	**E-mail does not use your name**	A form of address that does not use your name (e.g. just “Hello” or “Dear costumer”) can be the first sign of a phishing or scam attempt.
☐	**Sender’s e-mail address**	Criminals use e-mail addresses that do not match the e-mail addresses of real companies or institutions, but they may look very similar. They often use the names of well-known companies at the beginning of their e-mail address so that the recipient thinks this is the sender. The underlying account is a fraudulent website.
☐	**Urgency**	Phishing and scam messages urge the recipient to act fast to prevent further damage, like their account being blocked, their subscription being canceled (e.g. with online streaming platforms) or missing out on a bargain. Such pressure is supposed to make you click on links and provide information without thinking twice.
☐	**Links leading to suspicious websites**	Don’t click on links in messages and e-mails as they may lead to fraudulent websites or malware. Think whether you know where exactly this message is coming from. If you are unsure, get in touch with your provider (log on to the app or the website as usual) and check whether they really require you to do something. If you suspect any fraudulent activity, change the password of the affected account immediately. You can also report suspicious websites at watchlist-internet.at.

☐	**Suspicious attachments**	Suspicious attachments often contain self-installing malware that forwards sensitive data from your devices to criminals.
☐	**Spelling and grammar mistakes**	E-mails from fraudsters often contain spelling and grammar mistakes. Sometimes the whole text is just a bad translation.
☐	**Incomplete company information**	Fraudulent online shops often do not have a disclaimer, copyright notice, information about consumer rights or contact details.
☐	**Premium-rate telephone numbers**	You can block premium-rate services from contacting your number. You can do that yourself in the app of your mobile service provider, or just call the service line. That is how you can avoid unwanted debits.