

How to recognize a digital scam



KULUTTAJALIITTO
KONSUMENTFÖRBUNDET

huijausinfo.fi

This training is designed to increase your knowledge and understanding about digital scams. After completing it, you will know the most common types of scams, how to identify them, and what to do if you get scammed. The aim of the training is to support and encourage the safe use of the internet.

You can use this training package either for self-study or for advising others. You can also share it with others in your network.

This training has been put together as part of the ‘Huijarit kuriin!’ (Taming the Scammers) project run by the Consumers’ Union of Finland and funded by STEA (2019–2021). More information about the project and about digital scams can be found at www.huijausinfo.fi

This training package was updated in December 2021.

The Consumers’ Union of Finland is open to all. It is unique organisation that promotes the interests of consumers and public service users nationwide as well as providing training and advisory services. We defend the rights of consumers and public service users within societal decision-making processes.

You can find out more and become a member by visiting <https://www.kuluttajaliitto.fi/en/become-a-member/>.

978-952-9787-74-6 (print)

978-952-9787-75-3 (pdf)

Content

1. General information about digital scams	4
2. E-commerce scams and subscription traps	6
3. Scam messages and phishing	11
4. Technical support scams	17
5. Online romance scams	19
6. Investment scams	23
7. CEO scams	27
8. Instructions for scam victims	28
9. Further information on scams	30





1. General information about digital scams

Digital scams cover various types of fraud committed by criminals using digital devices (such as computers, tablets or mobile phones) and aimed at obtaining the victim's money, personal information or passwords.

Behind these scams are often international networks of organised crime. Even if Finnish is used in the scam, this does not mean that it is being committed in Finland. A large proportion of scams are carried out outside of Finland's borders.

The aim of scams is to obtain economic benefit either immediately or by using the information obtained from the scam at a later stage.

Digital scams can be categorised in the following way:

- E-commerce scams
- Scam messages
- Technical support scams
- Online romance scams
- Investment scams
- CEO scams (not only companies but also associations and organisations)

The basic rules for safe internet use

- Be careful and always think about what you're doing.
- Don't make decisions in a hurry. Scammers usually try and pressure you to act carelessly by threats or by creating a sense of urgency.
- Be critical – don't believe everything you find on the internet. If something seems too good to be true, it's usually not true!
- Check the details: site reliability, message sender, link addresses.
- Seek out more information and learn how to identify different types of scams.
- Ask for help if you're not sure about something. You can get help from libraries and digital support staff, for example.
- Do not access an online bank or an official online service via a link from a search engine or email!
- Do not open a link from a strange number or address!



2. E-commerce scams and subscription traps

E-commerce scams

Nowadays, you can buy almost anything online. In addition to reliable online shops, however, there are also scam websites and scam advertisements. There are also scammers on online second-hand stores (Tori.fi or Facebook, for example) who may pose as buyers or sellers of second-hand goods.



Do not make purchase decisions in a hurry! Consider and check the reliability of the online store by using, for example, a search engine.

In e-commerce scams, criminals create sites that look like a real online store to cheat people out of their money.

In online second-hand stores, scammers use fake personal information.

Scam online shops sell all the different services and goods that people might want (e.g. clothing, timeshares, rental cottages, telephones).

How to avoid e-commerce scams

- Remember that nothing on the internet is free! The scammer will try to fool you with incredibly good offers and push you towards making a quick purchase decision.
- Make purchases from familiar companies or make sure the online store is trustworthy and reputable. You can do this by using a search engine (e.g. Google) to find comments from other users about the company and by making sure the online store provides enough information about the business running the store.
- Do not buy anything if you are unsure about the trustworthiness of the online store.
- Always pay by credit card if possible. If you pay with credit card, you can then turn to the bank that issued the credit card if you get scammed and if it is not possible to resolve the issue with the online store.
- Save order confirmations, all communications with the vendor, and the vendor's acknowledgement of payment once the purchase has been approved.
- Read the terms and conditions carefully, including the small print.

Scammers can pose as familiar Finnish companies. In addition, there are a lot of fake accounts nowadays, especially on Instagram, which claim that a person has won a lottery and is now eligible to order or buy a product.



EXAMPLE



The screenshot shows a scam ad made in the name of the company chain Gigantti, claiming that the reader has won an electric scooter. The link for claiming the prize takes the person to the scam page.



This screenshot shows a social media channel on Instagram with a fake account and a post claiming that the users listed in the image have won a hair-dryer. The purpose of the scam was to direct the user to a scam page aimed at obtaining the person's credit card information.

Before purchasing, always check that the company clearly provides the following information on its website, especially if it is an online store that you have not used before

- Company information and contact information (company name, postal address, telephone number and e-mail address)
- Content and price of the product or service (including delivery costs)
- Terms of delivery, with particular attention to any product restrictions or abnormal terms
- Delivery method and delivery schedule of the goods or services
- Is it a one-time order or does it involve committing to a subscription?
- How the payment is made and under what conditions
- How to cancel the order or stop use of the service after purchase
- What warranty and service conditions apply to the ordered product.

Subscription traps

A subscription trap involves a consumer being tricked into committing to a subscription without realising they are doing so. These scams can be carried out by phone, through an online store or via scam messages.

The scammers may claim to offer a free sample, a free introductory offer, or participation in an online draw, but in reality the victim is caught in an subscription trap. If calling by telephone, the caller may tell you they are carrying out a market research study and that by participating you can get a product for just the postage cost.

Under the pretext of the product being offered, the consumer is tricked into committing to a long-term, fixed-term contract to order a good or service, without the consumer understanding or knowing that this has happened.

Scam messages sent in the name of the Finnish Postal Service, for example, have also led to people being caught in a subscription trap when they thought they were just paying a postage fee. In fact, the person has unwittingly committed to an 'order' that charges a certain amount to their account each month.

In a subscription trap, it is usually not possible to contact the seller's customer service to resolve the issue. As a result, cancellation of the subscription trap is usually not possible, and the charges may be difficult to stop.

Instructions for victims of subscription traps

- Pay only for what you have ordered! It is a good idea to check your account regularly for any unfamiliar charges.
- A consumer cannot be required to pay for, return or store a product or sample that has been delivered without an order being placed.
- A complaint must be made to the sender about the unordered product and accompanying invoice.
- Contact your bank if you notice any strange direct debits from your account or credit card.
- The website of the Finnish Competition and Consumer Authority (KKV, www.kkv.fi/en/) provides instructions on how to file a complaint. KKV's Consumer Advisory Services can assist with making complaints. Using KKV's complaint assistant, you can also make the complaint yourself (www.reklamaatioapuri.fi/en).



3. Scam messages and phishing

Scam messages are the most common form of scam. Almost everyone gets scam messages. Scam messages are sent via email, text messages, social media channels and other applications.

Criminals attempt to use these scam messages to phish the receiver's bank and credit card information, personal data and user data (e.g. e-mail ID and password).

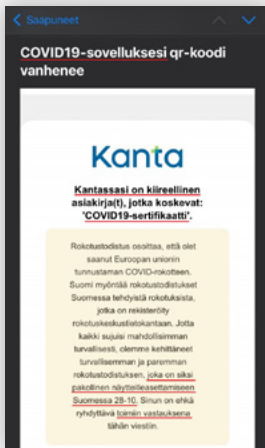
Scam messages are almost always accompanied by a link through which the victim is given further instructions. You should not open a link in an unexpected message!

On a smart phone, a scam message sent by SMS may go into the same message chain as genuine messages (e.g. Posti messages). This means it may be difficult to distinguish a scam message from a genuine one.

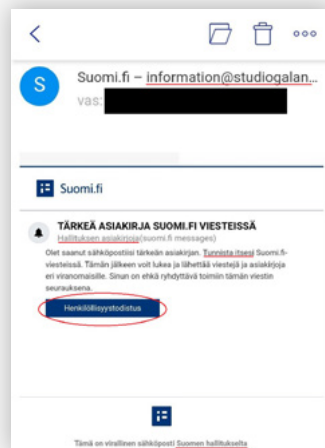
Scam messages may also claim to be from government authorities. These messages may claim, for example, that the Suomi.fi services, Kanta service or the Tax Administration service have a document for you that must be read through the link contained in the message.

There are also messages which claim to be from a Finnish bank and which threaten actions such as the closure of a bank card or online banking service if the person does not update their information using the link provided in the message.

EXAMPLE



Scam messages were sent in the name of the Kanta service when the coronavirus passport was introduced in Finland. These attempted to direct the recipient of the message via a link to a scam page on which the criminals tried to obtain the victim's online banking codes. The message contains several spelling errors and unusual terms.



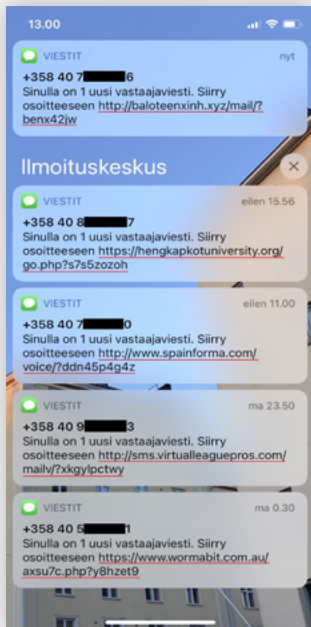
Scam messages are sent in the name of Suomi.fi services claiming that the recipient of the message has an important document in the service and must access it by using the link provided and identifying themselves with their banking codes. The message is used to direct people to a scam page that criminals use to access the victim's online banking codes. The message contains spelling errors, several unusual terms and suspicious claims about the sender.

In addition, scam messages may be sent in the name of businesses such as Posti, transport companies, shops and operators. The messages always try to pressure the receiver by creating a sense of urgency and threatening certain consequences if action is not taken.

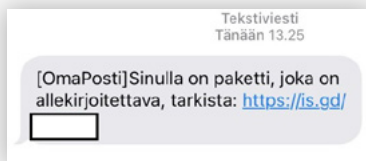
Scam messages are being sent in the name of all the banks in Finland. The messages attempt to threaten or intimidate – claiming for example that an account or a card will be closed – so that the receiver will act quickly and without caution. There is always a link to a scam page that looks like an online bank. The texts may use poor Finnish. For example, the message sent in the name of Nordea contained several typos and included threats to close an account.



- **Banks never use regular emails to ask their customers to update their information – only scammers do that!**
- **Messages sent by your bank are always found in your online bank under 'Messages'. If you receive a message claiming to be from your bank which asks you to do something via online banking, always go to the online bank either by entering the web address in a browser (e.g. www.pankki.fi) or by using the bank's own mobile application.**
- **Never open the link provided with the email or text message, download a strange message attachment, or provide your information unless you are not absolutely sure that the message is not a scam.**



Scam messages may arrive several times in quick succession. In scam messages claiming that the receiver has a new voicemail or package to sign for, there is often a strange, long link that leads to the scam page. The message appears to be from a Finnish number. Opening the link may download malware onto your device.



A scam SMS sent in the name of Posti alleges that the recipient has a package which must be signed for using the link provided in the message.

Blackmail scams

Scam messages can also be used to try to blackmail the recipient. The sender often claims to have hijacked the victim's computer or e-mail account and used the computer's camera to secretly film the victim.

Through the message, the scammer tries to extort money (usually cryptocurrency, such as bitcoins) and threatens to share 'sensitive' images with the victim's colleagues and other close friends.

This is simply a scam, and the machine (usually) has not been hacked or hijacked. Never pay the money demanded by blackmail messages. Report the blackmail message to the police.

Identifying a scam message

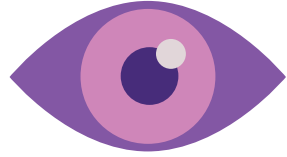
Before reacting to a message you receive, consider the following:

- Is the message trying to pressure you into acting by creating a sense of urgency or threatening serious consequences?
- Do you know the sender?
- Does the message contain a link that must be used to deal with the matter?
- Are there spelling errors in the message?
- Is the message content suspicious in some other way?
- If the message contains a link, does it look strange?
- Would the organisation in question contact you in this way with this kind of message?
- Does the offer or prize draw in the message sound too good to be true? Or do the consequences mentioned in the message sound too bad to be true?

What to do if you receive a suspicious message

1. Do not open any strange-looking links in the message.
2. Do not log in to online banking or government services via links provided in messages.
3. Go to the service that the message claims to be from by entering its web address into a browser's address bar (e.g. www.pankki.fi for an online bank)
4. If you do not know whether the message is a scam or not, you can ask about it by calling the customer service of the company that the message claims to be from. Do not reply to the message directly, however, but rather separately look up the contact information for the customer service. Companies usually announce any prize draws and competitions on their websites. You should check whether the competition or prize draw mentioned in the message is real.





4. Technical support scams

In a technical support scam, a criminal calls someone, impersonates a technical support person, and claims that the person's computer is under threat. Usually it is an English-speaking scammer saying that they are calling from Microsoft technical support and claiming that:

1. they are calling from the Microsoft head office where the person's computer has been monitored,
2. the victim's computer is sending out some kind of signal of a fault that needs to be fixed,
3. the computer has been infected with malware and accounts may have been hijacked,
4. the situation is urgent and only they can help save the person's computer.

The caller wants to give the impression that this is a matter of extreme urgency and that it is essential to listen to and follow his instructions.

Usually, the scammer asks the victim to download remote access software to their device that will allow the caller to help regain control of the machine.

If you receive a technical support scam call

1. Hang up immediately. **Neither Microsoft nor anyone else does any monitoring of consumer devices or provision of general technical support.** Technical support is a service that is used by some companies, for example, but Microsoft does not provide such a service.
2. Never download remote access software or other applications to your device if you are not sure what the program is used for. A person who calls you out of the blue and insists that you download a program is always a scammer.
3. Do not believe the caller, even if he claims to know the details of your device.
4. If you downloaded the remote access software or otherwise proceeded as instructed by a technical support scammer, report the matter to your bank immediately and have your device checked for malware by a professional.



5. Online romance scams

In an online romance scam, the impostor poses as a fictitious character with the aim of forming a romantic relationship or friendship between this non-existent character and the victim. The aim of the scammer is to use this kindled romance to get money from the victim.

The perpetrators of these crimes are highly-skilled in human psychology and use of data networks. They ruthlessly exploit people's natural desire for companionship and a soulmate.

By skilfully appealing to emotions, they can succeed in cheating people out of even large sums of money. Many victims of romance scams lose tens or even hundreds of thousands of euros.

Romance scams can end up being carried out over a number of years, and the victim may end up losing all their savings and even taking out loans.





The plot of an online romance scam

1. The scammer usually approaches the victim via social media (e.g. Facebook or Instagram) or dating apps (e.g. Tinder).
2. As a rule, communication is carried out through different messaging applications (WhatsApp, Hangouts, Messenger).
3. The scammer may tell you that they are working in a crisis area or on an oil rig
4. The impostor's social media profile often presents a handsome and wealthy officer or a beautiful actor from America or Eastern Europe. The pictures and the person's name, title, and life story are either made up or stolen from another person's social media accounts.
5. The scammer often says that they know a lot about Finland and that they want to come and visit. However, the visits to Finland are always cancelled due to different unfortunate turns of events.
6. Usually video chats don't work out and calls are only made occasionally.
7. Often the scammer claims that they have recently inherited or received a large sum of money or that they are already rich for some other reason. However, the scammer is for some reason prevented from spending his money and therefore asks the victim to 'lend' them money.
8. Often you are asked to make money transfers to someone else's account, not to the scammer themselves. Requests for money may also relate to some emergency, such as hospital expenses, payment of salaries, customs duties, unemployment, divorce or the death of a loved one.
9. The scammer may threaten the victim or make them feel guilty if they refuse or are unable to make the money transfers requested, and if the credibility of the person asking for the money is questioned, the scammer may pretend to be offended and angry.

10. The cheater seeks to prove his own trustworthiness and authenticity through methods such as sending pictures of themselves in which they are with animals or children or doing a job that inspires trust. The scammer may also present links to their company's website. They usually say they are wealthy, have a good job and are in good physical condition.

If you suspect the trustworthiness of an online acquaintance, ask yourself these questions

- Why would they be approaching me in particular?
- Do I really know who my online sweetheart is?
- Have I ever met them?
- Is it possible to communicate with them by phone or video?
- Do they ask me for money for supposed travel expenses or passport purchases, or because of different kinds of dramatic events and tales?
- Do these requests involve any pressure, urgency or blackmail?

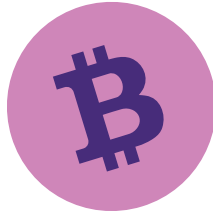


If something seems too good or too bad to be true, it's usually not true!

How to avoid online romance scams

- Be careful when getting to know people online. This is especially important if a complete stranger sends you a message out of the blue. Don't be too quick to believe all the stories your new acquaintance tells you.

- Check their background by, for example, searching for their name on Google and using Google's reverse image search. Try to verify the identity of your acquaintance.
- Do not send them money or pictures of your passport.
- Demand a face-to-face meeting and that they pay for their trip to visit you.
- Chat with the person using different communication channels. Today, everyone has the opportunity to make both video calls and regular calls.
- Talk to those close to you about your new acquaintance.



6. Investment scams

The investment scam involves drawing people in with the offer of a highly profitable investment which may involve purchasing shares, bonds or cryptocurrency, for example.

Often, this unique investment opportunity is specifically offered to you. The offer is said to be valid for a short time only and comes with a promise of getting rich quick.

Scammers produce various fake online news items and advertisements using images of trusted Finnish celebrities and public figures who are alleged to have become rich by investing in virtual currency or who recommend Bitcoin investments (e.g. Matti Rönkä, Mika Anttonen, Sauli Niinistö, Sanna Marin, and Ville Haapasalo)

Investment scammers also advertise on Tinder and via search engines such as Google.

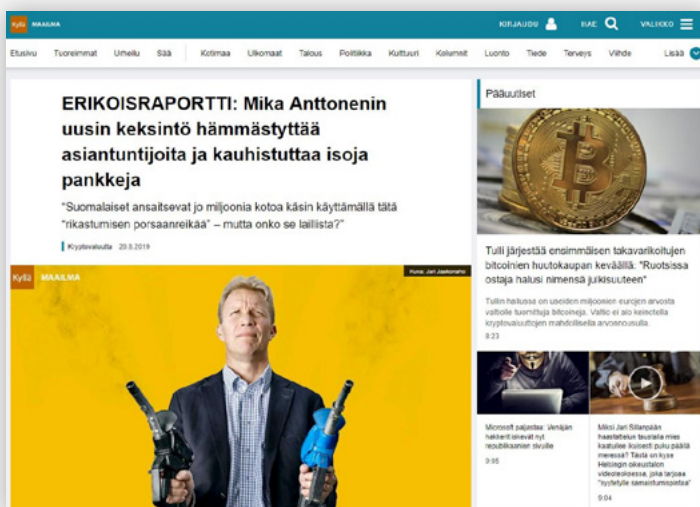
For the victims, investment scams often involve large losses, ranging from tens to hundreds of thousands of euros.

The plot of an investment scam

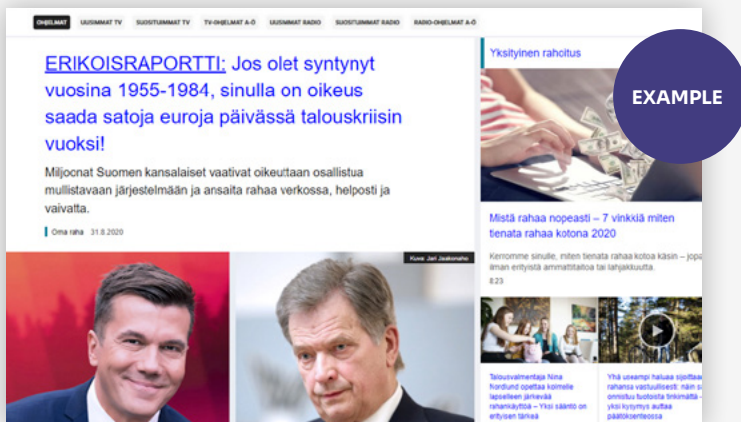
1. The investment scam usually starts with a fake advertisement, seen on social media, which advertises highly profitable investment opportunities that should be taken right away because the opportunity will soon be gone.
2. The ad leads to a scam page which may be made out to look like an Yle News website, for example. This page provides detailed instructions on how to make the investment. Once a potential victim provides their contact information, the scammers start pressuring them in order to try and get as much money out of them as possible.
3. The victim is tricked into investing money in something that does not actually exist.
4. They then receive calls and emails asking for an additional investment via a foreign bank account or virtual currency exchange service.
5. The victim is always offered higher profits and the 'evidence' provided is fake stock market charts or websites that show that investments are doing well.
6. The victim may be asked to install on their computer remote access software through which the investment vendor claims they can provide a better service. In reality, the scammer uses this to make unauthorised transfers from the victim's bank account, possibly even clearing out the victim's entire account.
7. The calls and messages may come very often and may be aggressive in tone, and you can't withdraw your own money even if you want to withdraw your investment or the 'profits' you have obtained.

For investment scams, a fake news page is often created to advertise the scam using the face of a familiar Finnish celebrity or public figure. The pages are often disguised as Yle News pages, for example, and contain detailed instructions on how to make the investment as well as advertisements for cryptocurrencies. Often there are typos on the pages, and the links to other articles usually do not work. The scam pages are advertised via channels such as Facebook and Google.

EXAMPLE



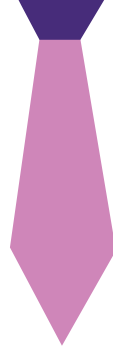
An investment scam is often made by creating a scam page that is advertised in social media. This example is designed to build trust in cryptocurrencies and the scammer's service, as well as providing details on how to invest. The name and image of CEO Mika Anttonen were used on the scam page.



Scams have also used the image and name of President Sauli Niinistö to market a non-existent investment. This scam page, disguised as an Yle News page, claims that Finns of a certain age have a special right to invest in an advertised cryptocurrency, which is in fact a scam.

If you think you might be dealing with an investment scam

- Keep in mind that no one offers highly profitable investments or investment tips over the phone to ordinary people for free. Only scammers call and offer an investment opportunity.
- Don't invest your money based on an ad you've seen online (e.g. Facebook).
- Verify the background and reliability of the investment and the company handling it. You can ask for help from your own bank, for example, if you are not sure if the investment is genuine or a scam.
- Don't invest in things you don't understand. Particular care should be taken when investing in cryptocurrencies, as they are connected with a lot of scams and involve a lot of risks.



7. CEO scams

A CEO scam is directed at a company, association, or organization or an employee of one of these.

In this scam, a criminal poses as a top manager from your organization who either asks you to transfer money abroad under some pretext or first asks for the organization's bank account balance and then asks you to make a transfer.

The scammer insists on the urgency or sensitivity of the matter and in various ways puts pressure on you to make the payment.

Usually, the scammer sends an e-mail in the name of a person in a management position. The email message may appear to come from the manager's email address, even if it wasn't sent by them.

If there is anything suspicious about the message, or if its content is very unusual, check the matter by first calling or sending an email to the person in whose name the message came.

Never reply directly to the message sent, but instead send a new message in order to ensure that your question goes to the intended person and not to the scammer!



8. Instructions for scam victims

If you have lost money, personal data or banking IDs

1. Contact the customer service of your bank as soon as possible and tell them about the scam. Your bank may block your bank account and your debit and credit cards if the details of them have been obtained by a scammer.
2. Report the crime to the police at www.poliisi.fi/en/

Get help from others

Do not just deal with it on your own! Talk about the scam with those close to you. You can also talk to someone about the scam by calling Victim Support Finland (www.riku.fi/en/).

The Finnish Competition and Consumer Authority can assist in investigating the scam if a Finnish company is involved (www.kkv.fi/en/consumer-affairs/).

In cross-border trade within the EU, you can get help from the European Consumer Centre Finland (www.ecc.fi/en/).

Voluntary credit bans and blocking direct marketing on your phone

If your personal data has been stolen by criminals through a scam, you can purchase a two-year voluntary credit ban

- This credit ban prevents you from making any purchases on credit.
- The ban can be cancelled if needed
- There are two service providers for this in Finland: Suomen Asiakastieto Oy and Bisnode

Blocking direct marketing on your phone

- Direct marketing can be restricted by registering for a direct marketing restriction service. These services may be subject to a fee.
- More information is available on the website of the Finnish Competition and Consumer Authority at www.kkv.fi/en/.

Dealing with the shame of being scammed and supporting a scam victim

A scam victim is a victim of fraud – there is no need for them to feel ashamed.

Being scammed can be compared to experiences of abuse, as victims of abuse also experience shame. Usually the victim of a scam blames themselves for the scam.

The most important thing in dealing with this shame is to talk about the scam and seek professional help if needed. When a person already feels ashamed, they should be treated very gently.

9. Further information on scams

Consumers' Union of Finland databank on scams

www.huijausinfo.fi

Police

poliisi.fi/en/being-scammed

Victim Support Finland

www.riku.fi/en/various-crimes/an-online-scam-can-happen-to-anyone/

The National Cyber Security Centre at the Finnish Transport and Communications Agency Traficom

www.kyberturvallisuuskeskus.fi/en/

Consumer Advisory Services of the Finnish Competition and Consumer Authority

www.kkv.fi/en/consumer-advice/

European Consumer Centre Finland

www.ecc.fi/en/

Public Service Info provided by the Digital and Population Data Services Agency, tel. 0295 000

Warnings about current scams can be found on huijausinfo.fi and on the websites and social media channels of the National Cyber Security Centre and the police

Scam information

on Twitter and Facebook @huijausinfo

The National Cyber Security Centre

on Twitter @CERTFI and Facebook @NCSC-FI

The police

on Twitter and Facebook @Suomenpoliisi

Scan warnings can also be found in the
112 Suomi application

Materials about scams from Yle's 'digital workouts' (in Finnish):

Scam quiz: <https://yle.fi/aihe/artikkeli/2019/05/17/digitreenit-testaa-parjaatko-nettiajan-huijareille>

Can you recognize a trusted online store: <https://yle.fi/aihe/artikkeli/2021/01/30/digitreenit-tunnistatko-luottävän-nettikaupan-testaa-9-kinua>

The website and YouTube channel of the Consumers' Union of Finland feature several training videos on scams

www.huijausinfo.fi or
www.youtube.com and search for 'huijausinfo'

You can read more about scams at huijausinfo.fi

huijausinfo.fi



KULUTTAJALIITTO
KONSUMENTFÖRBUNDET