

Scamaware – in brief

It can be tough to see through convincing scammers who are trying to trick you. Here are three tips to reduce the risk.

- 1 Hang up if the conversation starts to feel uncomfortable, stressful or strange.
- 2 Don't use your bank security device or electronic identification (like BankID) to log in at somebody else's request.
Don't tell anyone your passwords or security codes.
- 3 Your bank will never phone you to ask you to log in or to provide personal details.

- Have you been the victim of fraud? Contact your bank immediately!
- Always report attempted fraud to the police. Ring the police on 11414.

Write the phone numbers of your bank and a family member here:

More and more people are being targeted by fraudsters, and there is a huge need to raise awareness about this broadly among the general public.

Scamaware! is an initiative by Sweden's banks and the Swedish Bankers' Association. The purpose of this initiative is to provide useful advice and information about how we can protect ourselves and our family members from scams and fraud.

Contact your bank if you have any questions about security. Read more at svarlurad.se

**SVÅR-
LURAD!**
ETT INITIATIV AV
SVERIGES BANKER

**SVÅR-
LURAD!**
ETT INITIATIV AV
SVERIGES BANKER

**It's simple to
be scamaware!**

A leaflet containing advice on how to protect yourself and your family from scams and fraud.

An initiative by Sweden's banks and the Swedish Bankers' Association.


Read more at svarlurad.se

How scammers may try to trick you

Attempted fraud is on the rise and scammers are constantly changing their methods. The more you know how the scams work, the easier it will be to protect yourself from falling victim to them. In recent years, it has become more common for scammers to ring up and claim to be your bank, the police, a company, a government agency or even a member of your family. Fraudsters can manipulate phone numbers to make it look like it really is your bank that's calling.

They may try to make you feel stressed, for example by saying that you have a problem that needs to be resolved immediately. Fraudsters will often emphasise that time is short.

Next, the scammer tends to offer help solving their invented problem and getting the situation sorted out. They may ask you to share a security code from your bank security device, to use your electronic identification (like BankID) or to approve a Swish payment.

 **Be suspicious** when somebody contacts you out of the blue! And remember, scams don't only happen over the phone. Fraudsters may also try to trick you via text messages, on social media or by using email. They may even knock at your door. Always think whether or not what you are being asked to do is reasonable – and never share personal information or security codes. Don't log in if you are even the slightest bit suspicious.

Fraudsters may say:

- They are **going to help you stop an existing scam** on your account or card
- They can help you with **your tax rebate**
- They can help you with **coronavirus services**, like vaccinations
- They can help you **recover money** that you have been scammed out of
- You have **won some money**
- A **family member** has got into a tricky situation **and needs your help**
- Your **computer has a virus** or some other problem that they say they can help you with
- You need to download **software to protect your computer from an on-going virus attack**

Be scamaware

It's simple to be scamaware – and everyone can learn how. You can always end a phone call that feels strange. Tell the caller you'll get back to them and hang up. Then ring your bank or a family member and explain what happened – seek help and support from somebody you trust. Here are some common warning signs to watch out for and some important information:


→ **Remember** that fraudsters may claim to be your bank, the police, a company, a government authority or they may even claim to be a family member.

→ **Are you expecting a call from your bank or the company the caller claims to represent?** If not, then be careful about what information you give out. Tell the caller you'll get back to them if you are unsure about the person calling.

→ **Hang up if the call starts to feel uncomfortable, stressful or strange in any way.**

→ **Never log in anywhere at somebody else's request. When using electronic identification** (like BankID), always make sure you read all the information about the service you are accessing and what you are agreeing to.

→ **When using your bank card reader**, remember to protect your PIN code and never share security codes with anybody else.

 **Remember!** Your bank will never ring you to ask you to log in or give out personal information.

Supporting your family members

You can help play an important role in sharing information and knowledge with those close to you. Talk to your family members about the risk of being scammed and how best to prevent this from happening.

Share your own experiences with others who might not have the same knowledge as you. This is an important safety net for anybody who is feeling unsure or concerned. Together we can help keep each other safe and secure.

Read more at www.svårlurad.se