Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Security department
Information security officer
Christian Nähl

2019-01-22

Common types of fraud – how to protect yourself

This is a list of the most common types of fraud. Learn how to avoid being deceived.

1. Message from the Division of IT
You receive a message from the Division of IT saying that Outlook has run out of storage space and you have to log in on a page that looks like an SLU page.

The sender's objective:
The sender gets access to your username and password, can subsequently log in to SLU using your identity and send spam "from" your account. Perhaps you also use this password for other services, both at work and personally.

How to protect yourself:
Check the login page address to ensure that it really comes from SLU. If you are unsure, contact the Division of IT and change your password if you accidentally logged in.

2. Whaling
Someone claims to be a manager/head of department, etc. and that they have the power to decide on financial issues. They want employees to transfer money quickly, often to a foreign account. The email looks like it has been sent by a responsible manager/head of department, and their email address looks correct. They might also ask for important, sensitive information from a person, research project or SLU.

The sender's objective:
To get the employee to transfer money or provide the sender with information.

How to protect yourself:
If you are unsure, call the person who has asked you to transfer money and check that they really sent the email. Email addresses are like postcards – they can be forged. To check if the address is correct, click on "Reply" and see what address comes up.

Mailing address: Mailing address
Street address: Street address
VAT no: SE202100281701
www.slu.se

Phone: +46 18 67 10 00 (switchboard)
Mobile: XXX-XXX
firstname.surname@slu.se

3. Calls from a foreign number

If a foreign number calls you, do not answer unless you are expecting a call. If you have a missed call from a foreign number, do not call it back. The call is probably a fraud attempt. You risk losing a lot of money.

4. Message from your bank

Scenario: You receive an email or get a call from your bank saying that there is a problem with your account and that you must submit your account information. You are encouraged to do this – otherwise, your assets will be frozen pending investigation. The sender wants you to reply to the email and provide your information, or click on a link in the email. The link goes to a page where you can enter your account information.

The sender's objective:

To get you to submit your account information and get hold of your money.

How to protect yourself:

Banks and other financial organisations never request your information via email. If you are unsure that the message comes from your bank, call and ask. Never clink on links in this type of email. There is a risk that your computer will be infected with malicious software. The same thing goes for emails that claim that you have won the lottery, paid too much on an invoice or where a lawyer contacts you regarding inheritance from a previously unknown foreign relative.

5. False emails regarding tax refunds

Scenario: You receive an email that says that you are entitled to a tax refund. The sender claims to be the Swedish Tax Office.

The sender's email address can be refund@skatteverket.se, skatt@skatteverket.se or similar. You are asked to clink on a link that appears to go to the Swedish Tax Office.

The sender's objective:

- To get you to submit your account information and get hold of your money.

How to protect yourself:

- Never clink on links in this type of email.

This type of fraud is called phishing.

6. Calls from Microsoft support

Scenario: Someone who claims to work for Microsoft or Windows support calls you. They say that your computer has a virus, etc., and that you risk losing all data on your hard drive. They will then tell you to enter complicated commands on your computer, i.e. accept that they can control the computer remotely.

The sender's objective:

- To get access to data on your computer such as pictures, emails and account information.
- To download malicious software on your computer. This enables the sender to control your computer remotely and get access to your data. In addition, your computer can become part of a remotely controlled network (a botnet) used to attack other targets on the internet.
- They then demand that you pay for their service, often by asking for your card information. The payment is often drawn from your account several times.
- Access your account and bank information in order to make unauthorised transfers from your account.

How to protect yourself:

- Hang up the phone.
- Ask yourself if it is likely that a large IT company would call around, offering support.
- If you followed their instructions, definitely do not pay them any money.
- If the sender can control your computer, disconnect your computer from the internet. Ask an expert to check if anything has been downloaded to your computer.

7. Locked computer

Scenario: You are on the internet when a message from the police appears on your screen. You cannot close the message, and your keyboard and mouse stop working. The message states that you have committed a crime online. In order to unlock your computer, you must pay a sum of money.

The sender's objective:

- They want you to think that the message is from the police and that you should pay them.

How to protect yourself:

- Ask yourself if this is reasonable. The police never sends personal messages to internet users, especially those suspected of a crime.

- Unless you have ordered something or made an agreement with someone, never pay someone over the internet.
- Note that your computer may have been infected with malicious software when the message appeared. Scan the computer for viruses or ask an expert to see if the computer has any malicious software.

8. Letters from Nigeria

Scenario: You receive an email from someone who claims to have a large sum of money that they need help transferring from another country. The sender claims you will be rewarded if you help them.

The sender's objective:

- Trick you into a chain of events where you think you have to pay bribes and fees to receive your promised money.
- To get you to submit your account information. Your information is then used to access your money and to deceive someone else.

How to protect yourself:

- Ask yourself what the odds are that you of all people would be asked to take part of something that rewards great sums of money without barely doing anything?
- Never reply to these types of requests.

9. Romantic fraud, American military or deserter

Scenario: You receive an email from someone who claims to be a highly ranked military officer who works all over the world, or from an army deserter in another country. They send a picture of themselves with the purpose of developing a relationship with you. Once this has happened, they ask you to send them money so they can come and visit you in Sweden.

The sender's objective:

- Manipulate your emotions and get you to send them money.

How to protect yourself:

- Ask yourself what the odds are that someone, often from another continent, would contact you. The pictures they send as proof of existence are often downloaded from the internet.
- It is easy to search if the picture has been used in other contexts.
- You should also search their name.
- Never send money to someone who requests it online.