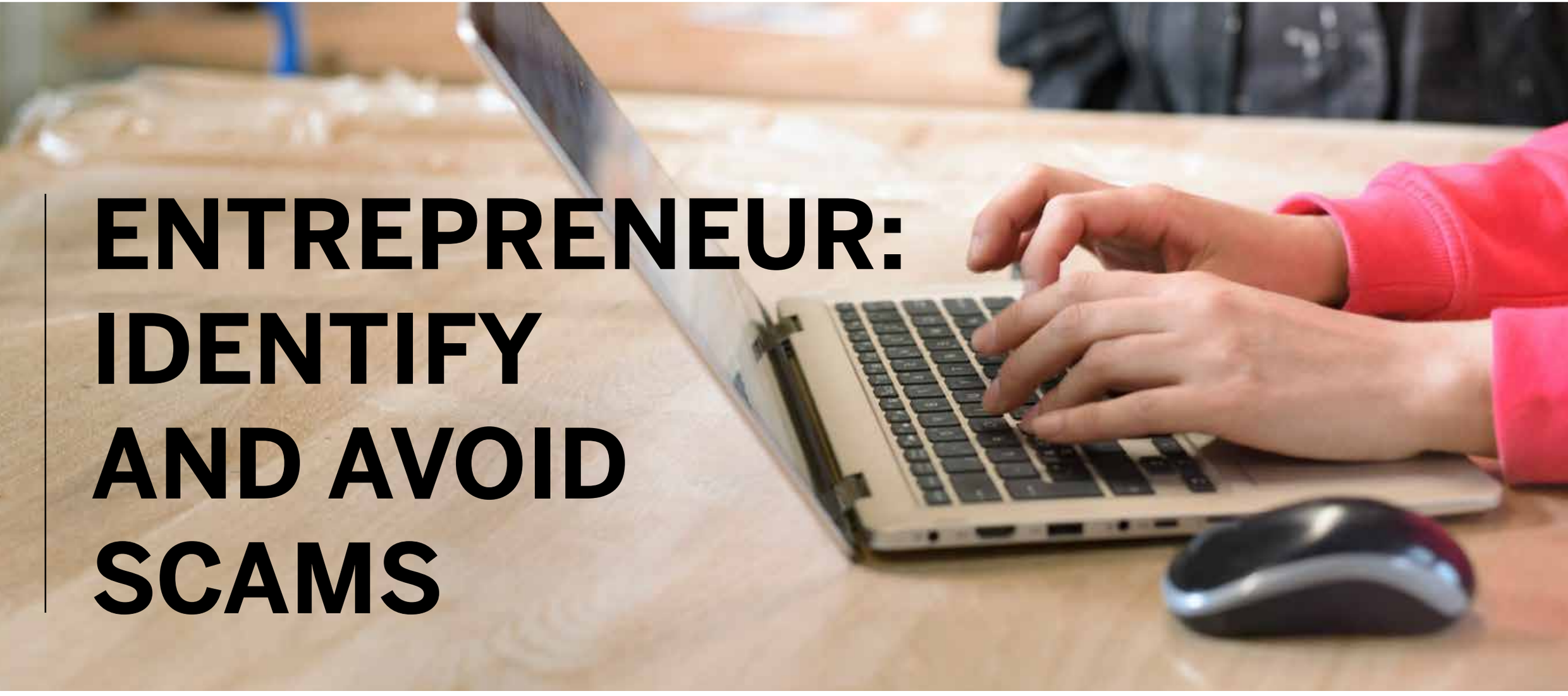
Yrittäjät



ENTREPRENEUR: IDENTIFY AND AVOID SCAMS

ENTREPRENEUR: THIS IS HOW YOU IDENTIFY AND AVOID SCAMS

Scams and criminal fraud aimed at businesses have increased significantly in the 21st century. Directory enquiry scams alone cost businesses €20 million annually.

This guide presents the most common types of scams directed at businesses. We also tell you what to do if you are the victim of attempted fraud or realize you have been defrauded.

Suomen Yrittäjät advises and helps its members in fighting fraud.

Yrittäjät

CONTENT

1 DIRECTORY ENQUIRY SCAMS

The most common form of misleading advertising is offering unspecified directory enquiry services. People who have just registered or bought a business, in particular, may find themselves the victims of multiple instances of fraud.

Telephone scams

A telephone sales representative calls a business owner and says he or she is updating information for a business directory. The salesperson may even claim to represent a reliable organization, such as a municipality.

The salesperson fails to mention at the start of the call that the service being offered comes with a price tag.
If the business owner gives his or her details to the caller, he or she hears only at the end of the call, "this service costs €X". That is when you should state you are not ordering the service, immediately on the phone or afterwards by email.

In spite of your refusal to order, you may soon get an order confirmation and invoice for the service by post or email

WHAT TO DO

- We recommend not placing any orders or making any agreements over the phone.
- Lodge a claim with the company immediately and demand to hear the recording of the call. Often this is enough to get the salesperson to back down.
- If reminder invoices arrive, you don't need to pay them.
- In spite of your claim, the salesperson may still outsource your file to a debt collection agency which then sends you a claim for collection. If this happens it is important to lodge a written or emailed complaint with the agency that refers to the lack of cause for the claim.
- It is a good idea to attach the claims you sent to the original invoice issuer to this new claim.
- It is extremely important to demand the debt collection be halted as a disputed matter and to deny the agency the right to use a commercial debt collection claim ("trattaperintä"), which carries the risk of a bad credit rating and the threat of publicity.

Directory enquiries claims by post and email

Businesses are contacted from abroad and asked for updated company details for a European business directory. The most well-known operator in recent years has been the European Business Network (EBN).

The upper section of the form contains columns for the company's details. Very fine print at the bottom of the page, amidst a long text, states that the service costs money. It may cost almost €1,000 under a multiannual contract that is difficult to cancel. Similar, Finnish operators have been active too.

WHAT TO DO

- You can ignore these "invoices" immediately. You do not need to lodge any claims related to them.

NB! READ THIS

Suomen Yrittäjät has put together a comprehensive information package on its website about misleading marketing and scam invoicing. The package contains information about typical forms of misleading marketing, and instructions for lodging claims, demanding telephone recording and dealing with debt collection agencies.

2 SCAM INVOICES

At its simplest, a scam invoice is a genuine-looking, completely baseless invoice which is used to attempt to make a business pay for a service or product it has not ordered.

Forged invoices

Fraudsters send an invoice in the name of a familiar sender, such as a cooperation partner or other company or organization known to the receiver. Logos and other identifying marks have been copied onto the invoice, making it look genuine. The account number, however, is the criminals'.

There have also been cases of invoices being stolen from companies' letterboxes. The criminals have entered their own account numbers on the true invoices.

WHAT TO DO

- If you suspect invoice forgery, always check the correctness and account number for the invoice with the organization marked as the sender. In the event of fraud, contact your bank and the police. You can prevent invoice forgeries by using e-invoicing.

Corporate debt collection claim threats

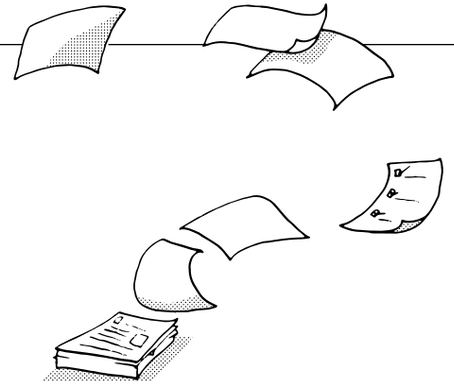
Companies have occasionally received invoices from suspicious debt collection agencies which state they are recovering the receivables of company X. The business owner receiving the invoice is threatened with tratta, or corporate debt collection claim, and the resulting poor credit rating. A pattern repeats in communications: the business owner has not been contacted before the tratta letter. This means they have received neither invoices nor reminders; the tratta letter was the first contact.

In recent years there have also been cases in which these tratta threats have been sent in envelopes of large, well-known agencies.

A tratta threat may read as follows: If the receivable is not paid by the due date, your credit rating will suffer. A poor credit rating will prevent you from accessing credit and damage your business opportunities in other ways. If the receivable is still unpaid, we will start legal recovery action, which will cause significant costs for you.

WHAT TO DO

- Do not pay. Invoices that are not based on a contract are baseless, nor do they need to be paid. See instructions in the comprehensive Suomen Yrittäjät information package.



Offers masked as invoices

These letters, generally in English, misleadlingly look like invoices but are technically offers for various products or services.

The information about the offer is included in the message in very fine print. The messages often state that the receiver is under no obligation if he or she does not approve the offer.

These scam invoices have been sent in the name of companies including Office World and Office Max.

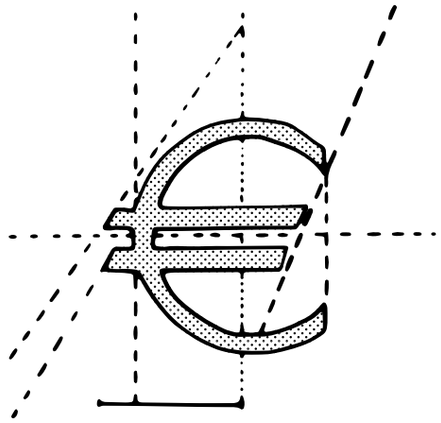
WHAT TO DO

- You can ignore these “invoices” immediately. You do not need to lodge any claims related to them.

3 CARD MACHINE SCAMS

Card machine scams are successful when scammers get their hands on chipand- PIN card machines. The scammer manages to find a menu on the machine which allows him or her to pay out a refund to the scammer's card, i.e., bank account.

Not all chip-and-PIN machines allow for the payment of such refunds. The risks are often bigger in small companies, for example in private shops or stall sales.



WHAT TO DO

- Block access to the refund menu. Card machines often have a menu which can be password-protected. You should without question set a password.
- Link the machine to a cash register system. These scams have affected standalone card machines that have not been linked to a cash register system. They cannot be carried out on system-linked card machines.
- Ask for the machine back as soon as the customer has entered the card and PIN. You should be suspicious if the customer spends a long time pressing keys.
- In unclear cases, contact your card machine provider.

4 TAX REFUND SCAMS

Fake tax refund notices sent by email are used to phish for credit card and bank account details.

The messages, bearing the Tax Administration's logo, are usually written in very poor Finnish: Dear taxpayer, when calculated tax operations for past year, decided, that you are entitled to tax refund €244.79.

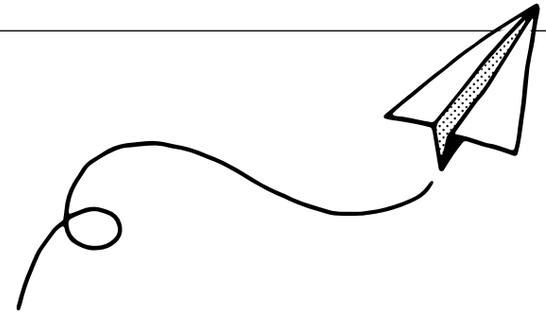
In the most recent fraud attempts, however, the Finnish has been almost flawless.

The Finnish Transport and Communications Agency recently warned about a large-scale tax refund scam. The recipient was told by email that he or she could receive a refund of €318.12 by registering on the "Tax Administration's" website and logging in with his or her banking codes. The scam page looked like vero.fi.

Bank icons directed the visitor to login pages which imitated those of Nordea, Danske Bank and S-Pankki. The pages asked for personal and bank details and said the visitor would receive a call within 48 hours.

WHAT TO DO

- You should delete such tax refund messages unopened.
- The Tax Administration has broad data receipt rights but it will never ask for account numbers or credit card numbers by email or text message.
- If you have given your credit card details to a scam site, you should cancel the card immediately.
- A scam message can also come in text message form. The Tax Administration reminds taxpayers- that it will never ask for personal details by text message, either.



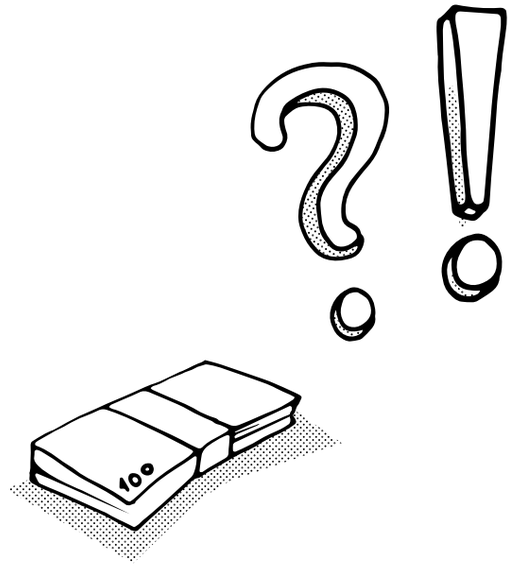
5 IDENTITY THEFT

The number of identity theft cases is growing fast. The costs to business from identity theft range from a few thousand euros to as much as hundreds of thousands.

Corporate identity theft is done by abusing open company data and cybersecurity breaches. There have been cases in which criminals have tried to capture a company by exploiting the paper form used to submit changes of contact details to the Finnish Patent and Registration Office (PRH).

The worst is if the criminals get their hands on personal identity numbers.

The company's details can be abused by ordering goods and sending the bill to the company, for example. The criminal may claim to be a company executive and change the company details in various administrative registers, try VAT refund scams – or even empty the company's bank accounts.



WHAT TO DO

- Make sure your personal identity number does not fall into the wrong hands.
- You should start using the PRH service which only allows for electronic notifications, or, at least, the alert service for changes to information on the trade register. https://www.prh.fi/en/companiesandorganisations/protect_yourself_from_scams.html
- By choosing the electronic-only option you ensure that only authorized people can notify the trade register and Tax Administration in the name of the company in future.
- Before signing for electronic notification, the Business Information System (YTJ) asks that you choose one of the following:
  - Only electronic notices are allowed.
  - Notices may also be received on paper forms.
- When you choose electronic-only notices, the trade register and Tax Administration will not accept paper forms (form Y) from your company any longer. The choice only affects notices which can be submitted electronically to the YTJ.
- Even if you have not switched to electronic- only notices, you will receive an automatic email about pending changes – such as the ones scammers make in attempts to capture the company.
- The company must have registered a functioning email address with the trade register for this automatic notification system to work.
- The other option is to sign an agreement with the PRH if you do not wish to provide your email address to the public trade register in fear of "peddlers". Such an agreement is free of charge.
- When changes occur in the registered information of the company being monitored, the trade register sends an email with a text file of the changed details within about an hour of the change being registered or the notificationbeing lodged with the trade register.

NB!

You can also take out insurance against identity theft from a range of companies and insurers.

6 VAT REFUND SCAMS

The Tax Administration has prevented hundreds of attempted fraudulent VAT refund claims in recent years, with 2016 being a real "boom". The most common scammers have been Estonian criminal groups, but there have been Finnish ones too.

The attempted scams have represented a total of tens of millions of euro.

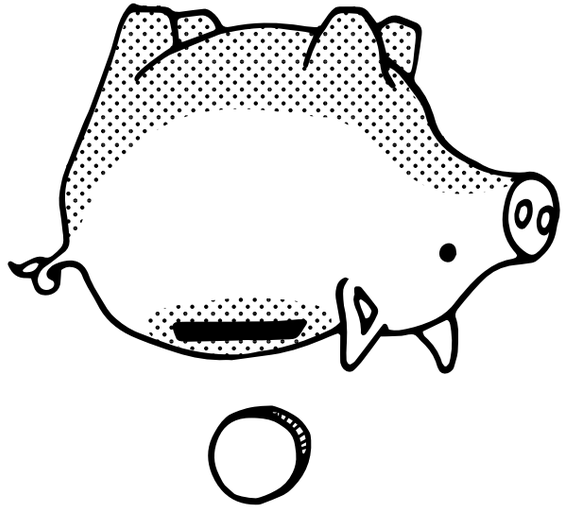
A VAT scam attempt usually proceeds as such: criminals provide the Tax Administration with a new account number in a company's name. After that they claim a VAT refund in the company's name.

The Tax Administration cross-checks these data and uses other analysis methods and "filters". In practice, the Tax Administration's success rate is 100%.

A couple of years ago the Tax Administration was forced to suspend the entire VAT refund system for a few days because of inspections of attempted fraud.

At that time the Administration contacted all companies that had submitted a change of account number, or those in whose name a change had been registered.

It paid particular attention to paper changes. The authorities encourage companies to do business with the PRH via electronic authentication.



7 CEO SCAMS

"CEO scams" are mostly targeted at large, internationally trading companies, but they have also been carried out or attempted with SMEs.

The criminals do careful background research on the company and its key people online.

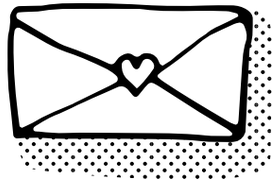
The scammers then send an email in the name of the CEO or other key person and try to make the staff responsible for payment make bank transfers to their accounts.

How the scam proceeds

The pattern in several scam cases is as follows: A criminal posing as a CEO, other director or lawyer sends the CFO, for example, an email with an urgent, confidential invoice for an acquisition or other urgent purchase. After this, the scammer posing as a company representative either calls or emails to say, "your CEO" (or other company representative) "has probably already spoken about this". Just as the CFO or person responsible for the company's invoices and payments is being confused by the call, he or she immediately receives an email supposedly from the CEO. The CEO asks in the email whether the lawyer has called and requests the invoice be paid immediately.

WHAT TO DO

- If you doubt the genuineness of the email, click reply. You should see the real email address.
- If the CEO's or CFO's email address is for example matti@yritys.fi, criminals might send a fraud email from matti@yr1tys.fi.
- The company's employees should be instructed to call the boss, even on holiday, in suspicious circumstances like these.



8 ORDER FRAUD

Order fraud is committed both in Finland and from abroad. The fraudsters take advantage of identity theft. Goods are ordered using forged identities and documents.

There have also been cases in which companies have been registered with the sole purpose of carrying out order fraud.

In traditional business-to-business order fraud the scheme is as follows: Initially small amounts of goods are bought from the seller and they are paid for as agreed. When trust has been established, the buyer places a very urgent order for a large batch of goods it has no intention of paying for.

Finnish companies have received large orders from abroad that have been skilful scams. In some cases, the scammers have even sent deposits – for example, cheques which end up bouncing.

Finnish online retailers have recently been the victims of scams in which the fraudulent buyer's visible IP address appears to be in Finland, but actually comes from a proxy server.

WHAT TO DO

- If the buyer is a company, find out as much as you can about it and its background.
- Always check the IP address to see if it is foreign, provided by a Finnish web operator, or that of a proxy server.
- The latter case has a clearly larger risk of a fraudulent order. A genuine buyer will not need to hide IP addresses or seek anonymity.
- You can check the ownership of an IP address onpublic databases such as: whois.com/whois/ ripe.net

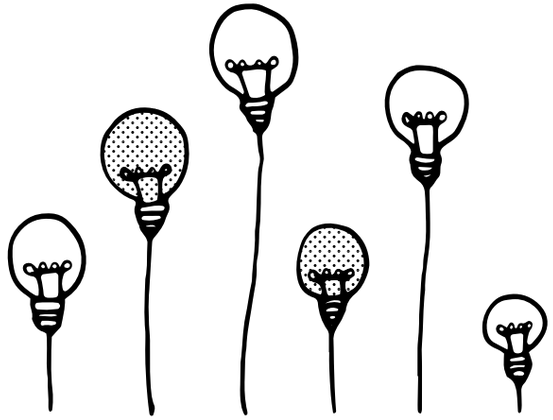
9 SCAM (PHISHING) EMAILS

These are emails with attachments that present a data security risk when opened. The emails are used to install viruses which are used to start char-ginga credit card.

Emails which ask for online banking codes are part of the phishing phenomenon, in which emails ask for and gather credit card details, account details and online banking codes.

WHAT TO DO

- Do not respond to suspicious mail. Do not in any circumstances open suspicious links or give personal, banking or credit card details by email either. In unclear cases, checking the information requests using an encrypted route, such as your online banking, is recommended.



10 OFFICE 365 SCAMS

There are scam emails in circulation bearing the Microsoft logo and company name which ask the recipient to click on the link in the email.

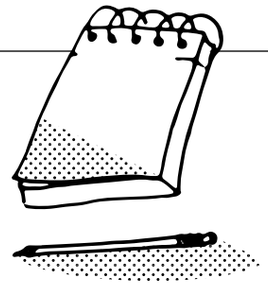
These scam emails say that to prevent the email account (usually a work account) from being locked, it must be verified by opening a link in the message and entering the account password. That is how the message senders try to phish for the account password.

The criminals have signed into companies' email systems using the Office 365 passwords they have phished. These frauds have caused many Finnish companies substantial losses and expenses.

If the fraudster gets into a company's email system, a hacker can set rules on the email accounts belonging to decision-makers or financial controllers or processors that make the email system send automatic copies to the hackers of all sent emails.

WHAT TO DO

- Check if your company's email system uses unauthorized forwarding rules and whether there have been logins to the company's data systems from strange places.
- Consider limiting the setting up of forwarding rules and adopting two-factor authentication.
- If you suspect a data breach in your company, you must file a crime report to the police on the matter.



11 TRADEMARK INVOICES

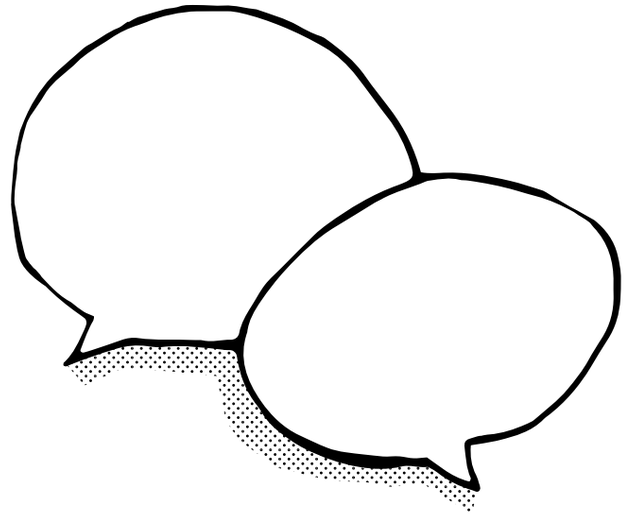
Companies applying for trademark protection should be vigilant, as there are quote letters resembling invoices in circulation.

They refer to genuine trademark registration numbers and urge businesses to pay a renewal fee. Many companies have mistakenly believed that the letters were sent by the PRH or the European Union Intellectual Property Office.

These “trademark invoices” generally bear official-looking EU star logos.

The PRH urges particular caution with letters that offer services related to trademark renewal or registered exclusive rights.

All notices and letters sent by the PRH clearly state PATENTTI- JA REKISTERIHALLITUS.

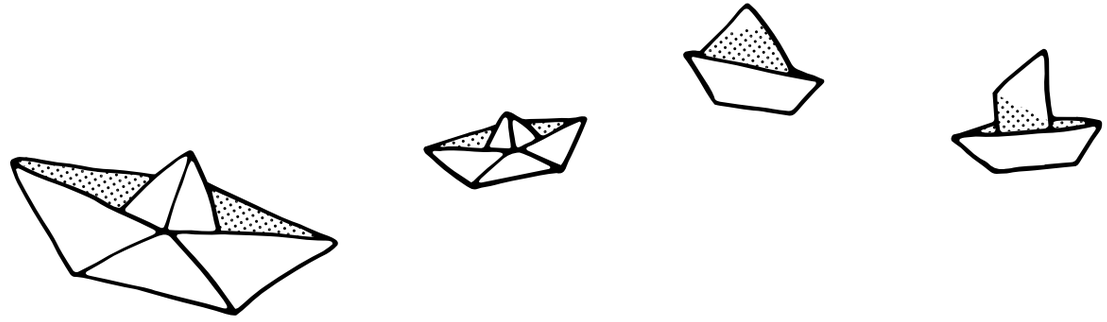


12 WEBSITE BUILDING SCAMS

Companies have been offered free website building, done by students. An invoice later arrives for work which was not ordered or done as a paid service.

The company may be scared by a telephone recording in which the construction of a website was ordered.

The number of these scams has declined in recent years, because it is easier to build a business website online using various website builders.



MORE INFORMATION HERE / LINKS

- **https://www.yrittajat.fi/tietopankki/liiketoiminta/harhaanjohtava-markkinointi-ja-valelaskut/**
- **kkv.fi/globalassets/kkv-suomi/julkaisut/selvitykset/2017/kkv-selvityksia-2-2017-pk-yrityksiin-kohdistuvat-huijaukset.pdf**
- **https://www.prh.fi/en/companiesandorganisations/protect_yourself_from_scams.html**

YOU CAN JOIN SUOMEN YRITTÄJÄT HERE:

yrittajat.fi/liity

Promoting enterprise.

Yrittäjät

KYLLIKINPORTTI 2, 00240 HELSINKI
PB 999, 00101 HELSINKI
(09) 229 221, TOIMISTO@YRITTAJAT.FI
WWW.YRITTÄJÄT.FI