



This project is funded  
by the European Union



Republic of Serbia  
Ministry of Trade, Tourism  
and Telecommunications



Republic of Serbia  
Ministry of Economy

# *How to deal with E-Crime?*

*E-BUSINESS DEVELOPMENT PROJECT*

**PROJECT:**

*E-business Development*  
[www.eposlovanje.biz](http://www.eposlovanje.biz)

**NATIONAL PROJECT DIRECTOR:**

Zeljko Rakic, Ministry of Trade, Tourism and Telecommunications

**PROJECT DIRECTOR:**

Sarah Shreeves, Exemplas Ltd.

**PROJECT TEAM LEADER:**

Leszek Jakubowski, Exemplas Ltd.

**PROJECT BENEFICIARIES:**

Ministry of Trade, Tourism and Telecommunications  
Ministry of Economy

**AUTHOR:**

Sinisa Begovic, short term expert, *E-business Development* Project

**EDITOR:**

Leszek Jakubowski

**CONTRIBUTORS:**

Branislav Veselinovic, Ministry of Interior  
Snezana Pavlovic, *E-business Development* Project

**PRODUCTION:**

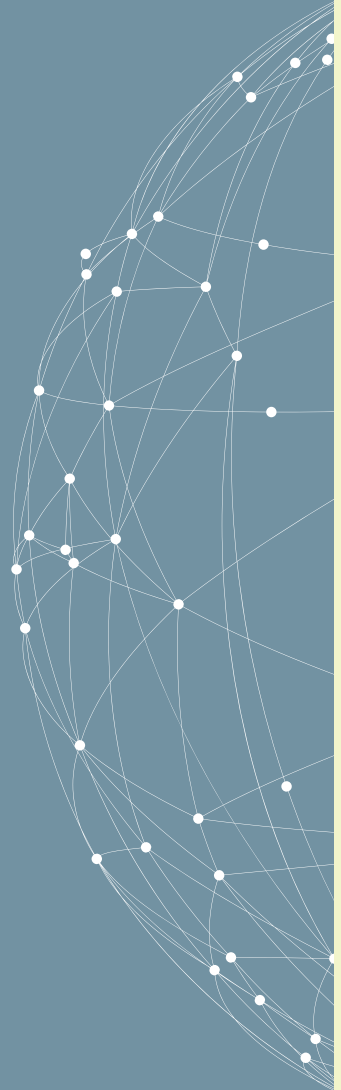
MaxNova Creative

**PRINT - RUN:**

100 copies

This publication has been produced with the assistance from the European Union. The contents of this publication are the sole responsibility of the *E-business Development* Project and do not necessarily reflect the views of the European Union.

The project is implemented by the consortium led by Exemplas, in cooperation with ACE Consultants, European Profiles, Imorgon, Seidor and Teamnet International.





# Contents

---

Introduction	5
1 Things you need to know	6
1.1 What is Electronic crime, e-Crime or Cyber Crime?	7
1.2 What is Identity theft?	8
1.3 What is SPAM?	9
1.4 What is Malware or Malicious software?	11
1.5 What is Firewall?	13
1.6 What is SCAM?	14
1.7 Trusted websites - What is e-Trustmark?	14
<hr/>	
2 Examples of Cyber Scams and frauds	16
2.1 Computer virus scams	17
2.2 Online trading scams	18
2.3 Banking and phishing scams	21
2.4 Computer hacking	24
2.5 Employment scam types	27
2.6 Investment scam types	29
2.7 Upfront payment scams	32
2.8 Mobile phone scams	34
2.9 Small business scams	36
2.10 Social media scam types	40
<hr/>	
3 Reporting e-Crime	44
<hr/>	

# Introduction

This guide deals with the demands of a rapidly changing digital world that results in an ever growing problem of e-crime. Its purpose is to help consumers and SMEs alike to become aware of the pitfalls and dangers in our constantly connected and networked environment where speed and anonymity of the internet leads to ever increasing cyber-criminal activity.

The guide sets out to increase the consumers and SMEs awareness of what to look for and what protective action to take. The right level of vigilance on behalf of the consumer and SME will deter possible criminal activity and drastically limit the attractiveness and effectiveness of such crimes. The guide deals with debit/credit card fraud, privacy and identity theft, computer scams amongst other things and is organised in a simple to read format giving the reader information and knowledge about the things to look out for when using computers, i-pads and smartphones.

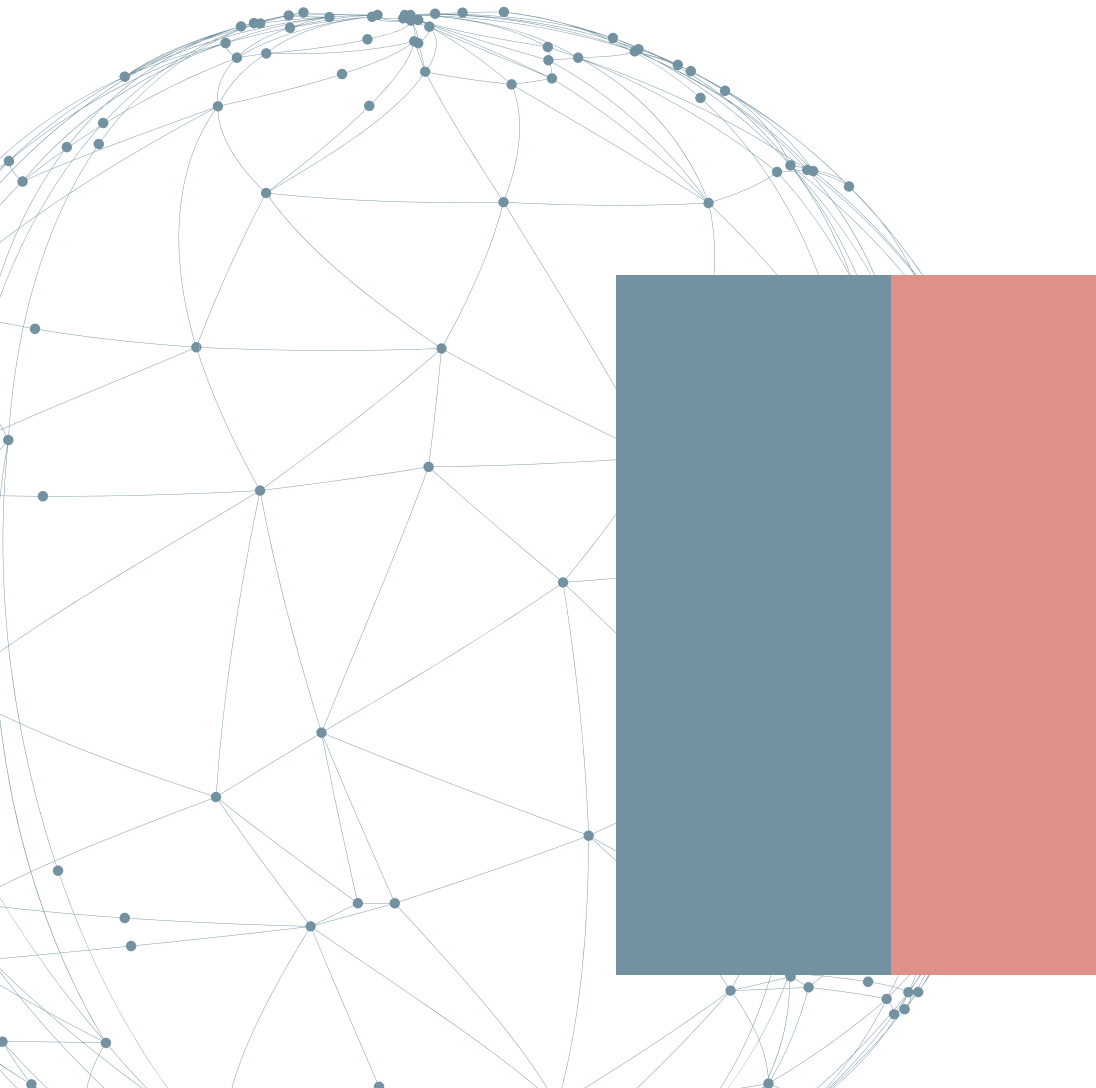
Section one deals with what the consumer and SME needs to know about e-crime.

It explains the basic terminology, elements and concepts that internet users need to know. At the end of each subsection there is a list of practical tips on how the consumer and SME can protect themselves.

Section two gives practical examples of cyber scams and frauds in order to familiarise the reader with potential dangers to look out for. This section explains to the reader in a practical way how to spot the potential activities of cyber-crime and how to react to it. As in section one each subsection gives practical tips of what to do to decrease e-crime vulnerability. In this way the consumer and SME will take a proactive stance in ensuring their own online security.

Section three is about reporting the e-crime. It directs the consumer to the Serbian institutions that can help or take action in order that the crime is not repeated. This section also provides contact details and web links to the institutions that can give help.

# 1. Things you need to know



## 1.1 What is Electronic crime, e-Crime or Cyber Crime?

Electronic crime, also known as e-crime or cybercrime, refers to criminal activity that involves the Internet, a computer or other electronic devices.

Some e-crime relates specifically to computers, such as distributing damaging electronic viruses or launching a denial-of-service attack which causes a computer system to deny service to any authorised user.

Other examples include fraud, harassment, copyright breaches and making, possessing or distributing objectionable material.

### *How to protect yourself against e-Crime?*

*Educate yourself about basic online safety and read this guide carefully.*

*Apply safety advice to all electronic encounters, including mobile phone use and texting.*

*Educate family members about basic online safety.*

*Set up basic protection against malicious software (malware) such as viruses and spyware on your computer.*

*If a business, ensure your Internet transactions and your customer/client information is secure.*

*If a business, establish a workplace Fair Use Policy and inform all staff about the policy by entering into individual use agreements. Monitor Internet use to ensure it follows your policy.*

*Fair Use Policy is set of rules applied by the owner, creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guide lines as to how it should be used.*

## 1.2 What is Identity theft?

Identity theft is when someone assumes another person's identity, such as their name, bank account details or credit card number, to commit fraud or other crimes.

Identity theft is one of the fastest growing areas of crime across the world and has no geographical boundaries – victims and offenders can be on opposite sides of the world. This makes it difficult for Police to investigate the crime, catch the perpetrator or help the victim.

The majority of identity crime is committed with the help of computers and other electronic devices. It can involve the theft of:

- *bank and credit card numbers*
- *addresses*
- *passports*
- *driver licence details*
- *names*
- *logon details for other services*





## How to protect yourself against Identity theft?

*Don't give out personal information over the phone, personally or via computers unless you are certain that the person or organisation you are giving it to is legitimate.*

*Never write your PIN numbers for your bank and credit cards on the cards themselves, or on any document or paper inside your wallet.*

*Dispose of personal information securely (shred papers, wipe/remove computer hard drives before sale or disposal).*

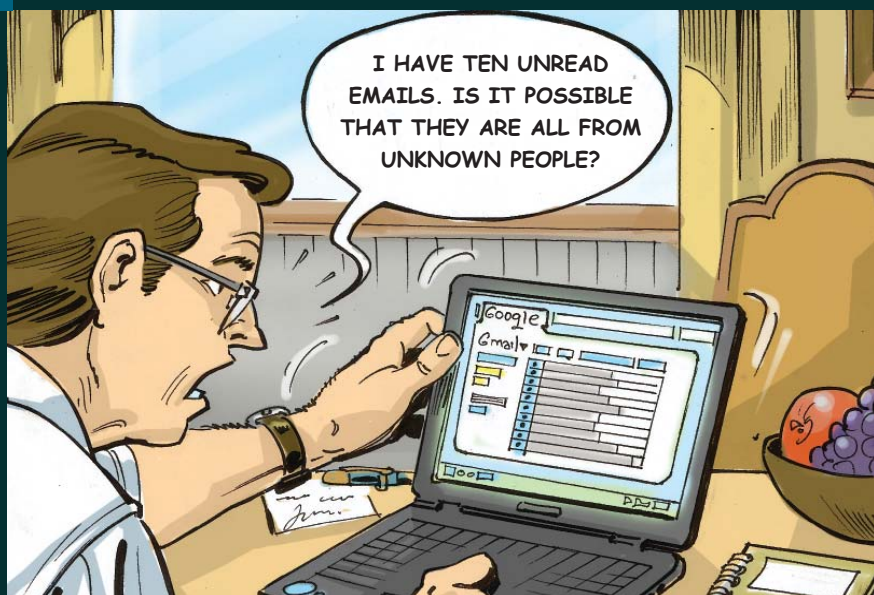
*Minimise the amount of identification documents that you carry around, including what you leave in your car on a daily basis. These are valuable items.*

*Check bank and credit card statements for unauthorised transactions. Report any discrepancies or unauthorised activity to the bank or card issuer immediately.*

*Be very wary of how much personal information you post on publicly accessible websites. Personal information can be misused in many ways by identity thieves, some of whom trawl websites.*

## 1.3 What is SPAM?

Spam is usually considered to be electronic junk mail or junk newsgroup postings. Generally, it is email advertising for some product sent to a mailing list or newsgroup. Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. It has become a major problem for all Internet users. The term spam derives from a famous Monty Python sketch ("Well, we have Spam, tomato & Spam, egg & Spam, Egg, bacon & Spam...") that was current when spam first began arriving on the Internet. SPAM is a trademarked Hormel meat product, well-known in the U.S. Armed Forces during World War II.



## How to protect yourself against SPAM?

### SCRAMBLE YOUR EMAIL ADDRESS

Rather than publishing your eMail address in its standard format, you could scramble and thereby conceal it. It requires an attentive and intelligent mind to recognize a scrambled eMail address and re-assemble it into a functional format. A scrambled eMail address can look something like this: *yourname at domainname dot com* and this is the unscrambled eMail address: *yourname@domainname.com*

### HIDE YOUR EMAIL ADDRESS IN AN IMAGE

#### ENCODE YOUR EMAIL ADDRESS

If you must post an active eMail link, for example to give people a quick and easy way to contact you, you can encode your eMail address in a way that is not readable by spambots, which extracts eMail addresses from websites.

Following web service can be of help: <http://hivelogic.com/enkoder/>

### HIDE EMAIL BEHIND A TEST

With a tool called *scr.im*, you can protect your eMail address by hiding it behind a simple test. At *scr.im*'s start page you enter your eMail address and the site will provide you with an ultra short scrimmed URL, along with custom HTML to share your eMail address on Twitter, Facebook, within HTML documents and in forums.

### DON'T SHARE YOUR EMAIL ADDRESS

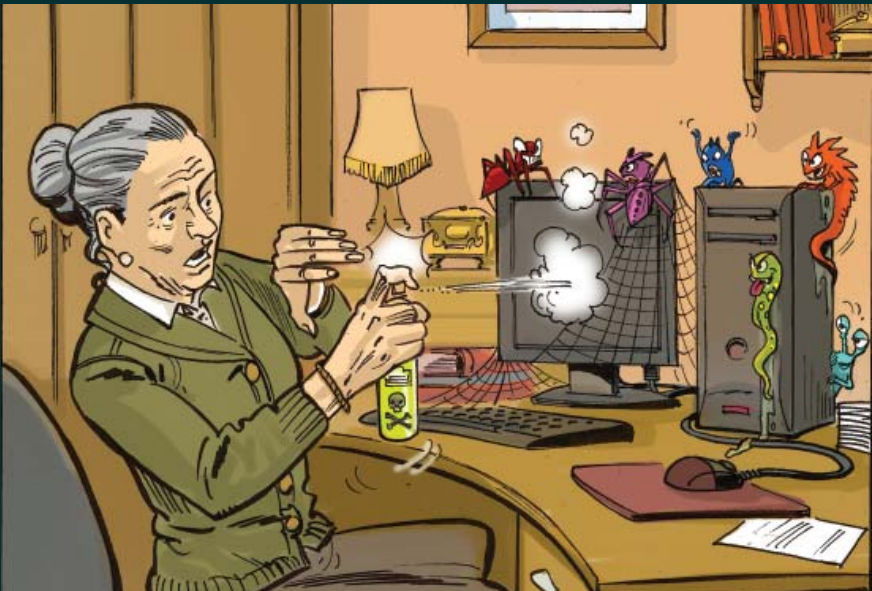
The last resort is to not share your eMail address at all. Set up temporary inboxes or forms through which you can be contacted indirectly. For example [www.whspr.me](http://www.whspr.me) allows you to create a temporary form, which will relay messages to your eMail address. Users have to prove they are human by passing a CAPTCHA test.

## 1.4 What is Malware or Malicious software?

Malware or malicious code are threats to computers and their security posed by spyware, viruses, worms, trojan horses and bots. They are very widespread programs that can record every key typed on a computer, capture screenshots, steal documents and files and open hidden backdoors to your computer. This information is then sent back to the person who installed it.

Malware can be installed by anyone who has access to a computer or they can be hidden in 'harmless' email attachments or uploaded via suspicious websites.

For example, if you use Internet banking, malware can record your bank account password. This information can then be used to remove money from your accounts.



# General classification of Malware

## VIRUSES

Viruses are small computer programs that can replicate themselves and spread to other computers. Some are relatively benign, simply displaying a message, but others are malign indeed, causing programs to run incorrectly, files to be destroyed and hard disks reformatted. Viruses are commonly classified as:

1. Macro: infect only the specific programs for which they were written.
2. File-infecting: infect executable files such as .exe and .dll files.
3. Script: written in scripting languages like Perl or VBScript.

## WORMS

Instead of infecting a relatively small number of files, worms infect whole computers rapidly. For example, the Slammer worm, which targeted a known vulnerability in Microsoft's SQL Server database software infected over 90% of Internet-connected computers within ten minutes of its release on the Internet, disabling supermarket cash registers and Bank of America cash tills.

## TROJANS

Trojans are malware masquerading as something the user may want to use or install that then perform unexpected actions, typically allowing backdoor access to the computer. Bots, short for robots, are malicious programs covertly installed on computers attached to the Internet. Unknown to their owners, these computers can then be controlled by third parties.

## SPYWARE

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as keylogging), passwords, and other valuable data.

## How to protect yourself against Malware?

*You don't always know whether you have malware on your computer, so it's important to have the latest virus detection software on your computer. Make sure that it checks for spyware. You should also:*

*Be aware that whenever you use a computer in a public place like an Internet cafe or library it may contain malware designed to capture your information.*

*Keep your operating system up to date.*

*Be careful with file sharing programs - if these are not configured correctly, others may have access to all your files.*

*Increase the privacy level on your browser to not accept cookies from untrusted sites.*

*Never click on a web link in an email, as they may not take you to the site they say they are.*

*Be careful when opening email attachments as they can infect your computer.*

*Be careful downloading programs from the internet, use a trusted source and virus scan downloads.*

*Be wary of websites that use popups or seem suspicious, as these can be dangerous.*

*Use a unique password for Internet banking that is different from all your other passwords.*

*Use malware detection software.*

*Set your web browser to not save passwords (and delete ones that may have already been stored).*

## 1.5 What is Firewall?

A firewall is a network security system, either hardware or software-based, that controls incoming and outgoing network traffic based on a set of rules.

Acting as a barrier between a trusted network and other untrusted networks a firewall controls access to the resources of a network and helps to screen out hackers, viruses, and worms that try to reach your computer over the Internet.

The most effective and important first step you can take to help protect your computer is to turn on a firewall.

If you have more than one computer connected in the home, or if you have a small-office network, it is important to protect every computer. You should have a hardware firewall (such as a router) to protect your network, but you should also use a software firewall on each computer to help prevent the spread of a virus in your network if one of the computers becomes infected.

## 1.6 What is SCAM?

As a term, scam is used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person. A scam is a quick-profit scheme where a person, group of people or organisation cheats another individual or group by presenting them with false information during a deal or offer.

Scams target people of all professional backgrounds, ages, education and income levels. There's no group of people who are more likely to become a victim of a scam, all of us may be vulnerable at some time.

Scams succeed because they look like the real thing and catch you off guard when you're not expecting it. Also, they exploit your desire to be polite and respectful, as well as your generosity and compassion.

Scammers are getting increasingly sophisticated in their attempts to get your money or confidential details. With the world becoming more connected thanks to the Internet, online scams have increased and there are many different types of scams.

We introduce the most common examples of scams under the chapter „Examples of Cyber Scams and frauds“, so you can recognise them on time and react properly.

## 1.7 Trusted websites - What is e-Trustmark?

E-commerce trustmark is an electronic commerce badge, image or logo displayed on a website to indicate that the website business has passed security tests and has been shown to be trustworthy by the issuing organization.

A trustmark gives confidence to customers and indicates to them that it is safe to do business with the web site displaying it.

For example, (<http://www.ecommerce-europe.eu/trustmark>) the Ecommerce Europe Trustmark stimulates cross-border e-commerce through better protection for consumers and merchants by establishing one European set of rules and by ensuring clear communication on these rules. Over 10,000 certified online shops can join the Ecommerce Europe Trustmark for free.



## 2. Examples of Cyber Scams and frauds





Cyber fraud has been around for just about as long as the Internet itself. Each year, cybercriminals come up with new techniques and tactics designed to fool their potential victims. You need to know what sets fraud apart from other Internet threats like viruses, Trojans, spyware, SMS blockers, etc: the target of the cybercriminals is not necessarily a computer, whose security has to be circumvented, but a human who, as we all know, has his/her own weaknesses. That is why no program can ever provide users with 100% protection; the users themselves have to take a proactive stance in ensuring their own online security.

This chapter was developed using many examples throughout the world from organisations such as Europol, UK Police, Serbian Police, FBI, Government Consumer Protection Departments of Serbia and New Zealand. It describes many different types of scams and frauds and gives advice on what action needs to be taken to protect yourself against them.

## 2.1 Computer virus scams

Computer virus scams are usually run from overseas call centres. You'll be called at home by somebody claiming to be from a technical support company. Windows or Linux Technical Services, PC Windows or Linux Support, Virtual PC Doctor are a few of the company names used.

The caller will tell you that your computer has a virus. They'll ask you to log on to your computer and to download a piece of software. This gives them remote access to your PC.

The caller will helpfully show you where the virus is on your computer. They'll then offer to sell you a six or twelve-month computer service contract. This is meant to protect you from any more viruses.

If you agree, the caller will take your credit card details. Or they may ask you to pay by electronic money transfer. What you don't realise is that there is no virus. The files the caller asked you to look at are a standard part of your machine.

What's more, the scammers may have downloaded spyware onto your computer. This gives them access to personal details like email address lists and bank details. The service contract gives you little or no computer virus protection. And you may find it difficult to get rid of.

I AM CALLING FROM WINDOWS HEADQUARTERS. YOUR COMPUTER HAS BEEN INFECTED, BUT WE ARE HERE TO HELP YOU SOLVE THE PROBLEM.



OH NO, HOW COME? PLEASE, HELP ME! SHOULD I SEND YOU SOME MONEY?



## What you can do to protect yourself?

*If someone calls you out of the blue to say your computer has a virus, just hang up.*

*If you've downloaded any software onto your computer, as a result of this scam, unplug it from the internet immediately.*

*You should also run spyware and antivirus programmes and change all of your*

*passwords, using a different computer. If in doubt, take your computer to a technician to be 'cleaned'.*

*If you've signed up to a service contract which you believe to be a scam, contact your bank or credit-card provider immediately. You may be able to get a chargeback.*

*Don't be intimidated by the callers, who can become very aggressive. Don't try to get any details from them. Just hang up.*

## 2.2 Online trading scams

### FAKE WEBSITES

It's surprisingly easy to set up a real-looking website. To help draw you in, scammers often use names and website addresses that are similar to those

of genuine retailers. For added credibility, they sometimes advertise in genuine online directories and on social networking sites. Or they may pay to be in search engines' featured listings.

Fake business pages on social media sites like Facebook can also be used to draw people into scams.

### **ASKING FOR MORE MONEY**

Some scammers advertise fake products then ask for even more money after you've paid. They claim to need extra payments for things like shipping, taxes and insurance.

As the original price seemed so low, you could be tempted to send the extra money. Don't. They'll keep coming up with reasons why they need more money. And for goods that didn't exist in the first place.

### **SCAMMERS ON GENUINE AUCTION WEBSITES**

Reputable auction sites have systems to spot scams. So scammers will often try to take you away from auction sites to do a deal. Be wary if anyone asks you for a private sale. Whether that's for one of their listings or something that you've listed.

### **FAKE ONLINE AUCTION SITES**

You could be directed to a false log-in site under the pretence of needing to restore your account, or verify your account details. Or you may get a message claiming to be the seller on an auction you missed out on. Over the course of several emails you'll be asked for financial and personal information that the scammer can use to steal your identity.

### **SENDING TOO MUCH MONEY**

Alarm bells should also ring if the person who wins your auction sends you too much money when it comes to pay. This is a type of Upfront Payment scam. The scammer will claim that they have made a mistake. They will ask you to send them a refund. Or they may ask you to forward money onto somebody else. Either way you'll find that their transaction is reversed and you end up minus funds.

### **FAKE TICKETS**

Scammers take advantage of major events like football games and music gigs. It's safer to buy tickets from authorised ticketing outlets.



## What you can do to protect yourself?

*Before buying online, it's a good idea to do your homework. Type in the company's name, followed by the word 'scam'. If the website is fake, you may uncover stories from people who've been caught out by the same scam.*

*Remember that comments about a company or product that seem too good to be true may be just that. It's very easy for scammer to write their own glowing reviews.*

*It's safer to pay by credit card than doing a bank transfer. If things go wrong, you may be able to get a chargeback. Be especially wary of sites that ask you to pay using a money wiring service such as Western Union. As a company you should never pay using Western Union or any similar service.*

*Check that payment pages look secure. Look for a padlock symbol and make sure the website*

*address begins with 'https' (the 's' stands for secure).*

*Always check out traders' contact details. Be on your guard if they only give you an email address or mobile number. If they provide a landline number, ring it. If you can't get through, or you're diverted to somebody in an overseas call centre, it may be a scam. Also be wary if the only address they give is a PO Box number.*

*Always read terms and conditions attached to any offer. Look for hidden costs and obligations. Don't trust offers that don't allow you to read the terms and conditions.*

*When trading on auction sites take into account the ratings given to buyers and sellers.*

*Resist suggestions to go outside the auction process to complete the sale.*

*Bank from invoice should be situated in traders origin country.*

## 2.3 Banking and phishing scams

### How banking and phishing scams work?

#### PHISHING

Scammers use phishing scams to trick you into handing over personal information. Information like your personal banking details and social media passwords can be very valuable to fraudsters. It gives them free reign on both your finances and your personal identity.

Phishing attempts are usually made by email. But they can also be over the phone, or by text.

#### CONVINCING REASONS

You'll be asked for your personal details – for example account number, log-in name, password, credit card or pin number. You'll be given a believable excuse for needing them such as:

- *Upgrading security*
- *System maintenance*
- *Verifying your account*
- *Protecting you from fraud*
- *Offering you a refund for a fee or a bill.*

Banks and credit unions do sometimes contact people about suspicious activity, but they will never ask you for your PIN number or passwords.

#### FAKE EMAIL FORMS AND WEBSITES

You'll be asked to fill in an email form, or directed to fill in a form on a website. The forms can look very convincing. They may have the same logo and format used by your bank or the company the scammers are pretending to be from.

Website names may be similar to, but not the same as the company's real website.

# Types of banking scams

## PERSONAL BANKING

You get an email from someone claiming to be your bank. It may look genuine, using the bank's logo and format. The email asks you to confirm your account details. You'll probably be given a link to a return email or website, where you'll be told to fill in your password and PIN number.

Don't. Banks will never ask you for your password or PIN number over the phone, in person or in an email.

Scammers send out phishing emails to millions of email addresses, hoping to hit real customers of a particular bank. So don't be surprised if you get a message from a bank you don't even belong to.

## MONEY TRANSFER SITES

You get an email from a money transfer site such as Paypal asking you to restore your account. The email may tell you that this is a security measure as your account has been accessed from another computer. You may also be asked to reload your credit card details onto the site.

## CARD SKIMMING

Scammers copy the electronic information from the magnetic strip of your credit or debit card at an ATM machine, or shop checkouts. Once they have your information they can 'clone' your card and access your accounts.

# What you need to know?

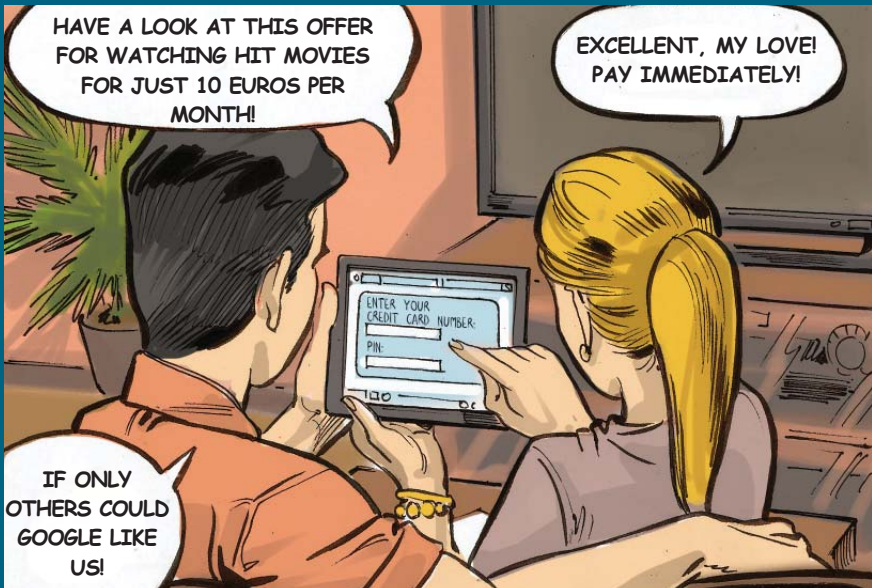
## WHEN BANKING ONLINE:

- make sure your computer has up-to-date anti-virus software and a firewall installed. Think about using anti-spyware software. Download the latest security updates, known as patches, for your browser and for your operating system
- before you bank online, ensure that the locked padlock or unbroken key symbol is showing in your browser. When a connection is secure, the beginning of your bank's internet address should change from 'http' to 'https'
- be wary of unsolicited emails - known as phishing emails - asking for personal financial information. Your bank or the police would never contact you to ask you to disclose your PIN

- ensure your browser is set to the highest level of security notification and monitoring. The safety options are not always activated by default when you install your computer.
- always access internet banking sites by typing the bank's address into your web browser. Never go to a website from a link in an email and then enter your personal details.

#### WHEN SHOPPING ONLINE:

- sign up to Verified by Visa or MasterCard SecureCode whenever you're given the option while shopping online. This involves you registering a password with your card company
- only shop on secure sites. Before submitting your card details, ensure the locked padlock or unbroken key symbol is showing in your browser. The retailer's internet address will change from 'http' to 'https' when a connection is secure
- never send your PIN over the internet
- print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number).



## What you can do to protect yourself?

*Never enter your personal details into a website unless you are sure it is genuine.*

*Check website addresses carefully. If they're similar to a genuine company's URL, but not quite right, be wary. Never visit your bank's website by clicking on a link - type in the website address yourself.*

*Don't give out account details over the phone unless you made the call and you trust that the number you called is genuine. Ask for a name and number so you can call them back, and check that number against a number you know to be genuine.*

*Don't reply to, click on any links, or open any files in spam emails. Don't call any numbers in spam emails.*

*Don't use software on your computer that fills in forms for you.*

*Never send your personal details or accounts or passwords in an email. Email is a very insecure system.*

*Check your account statements and credit card bill to make sure no-one is accessing your accounts. Order a credit report every year to make sure no-one is using your name to borrow money or run up debts.*

*Never let your card out of your sight at a store and say 'no' to requests to swipe your card through more than one machine. If you're worried about somebody's behaviour at a shop checkout, report it to the store's head office and contact your bank.*

*Don't use ATMs that have a suspicious device attached to its card slot. Report it to the bank immediately.*

## 2.4 Computer hacking

### SPYWARE

Spyware is a type of malware. When you click on links in spam emails, or download certain files from the internet, you can launch a spyware onto your computer, without realising.

Scammers use spyware to collect information about how you use your computer. For example, a 'keystroke-logger' is a piece of spyware that records every key stroke you make. So, when you visit your email, or internet banking, and type in your password, the scammer can see what you type.

Spyware can be hidden in files called 'trojans'. These seem innocent on the outside – for example an e-greeting card, a music files or an email from a 'friend' – but have dangerous programs hidden inside.



Once scammers have access to your computer they may:

- Collect personal information that they will use to steal your identity
- Use your computer to target other people with scams.

## Ways your computer hacking can be hacked

### **BANNERS AND DOWNLOADS**

Scammers use banners, pop-up windows, or even entire websites to install spyware onto your machine. They use free downloads, product trials or other offers to grab your attention. To claim your free stuff you need to click on a link. This installs spyware onto your computer. Sometimes you're asked for your credit card or bank account details, giving scammers valuable personal details there and then.

### **SPAM EMAILS**

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. Reputable companies don't send spam. So, when you get an unsolicited email, it's a safe bet to assume it is a scam.

Scammers use spam to:

- Trick you into handing over money or personal details
- Install malicious software onto your computer

Spam emails can have just about anything in the subject heading. They are used as a vehicle for many other scams and may invite you to do things like:

- Claim a prize in a competition
- Donate money to charity
- Buy discounted goods
- Make a lucrative investment

Spam emails are used to phish for banking passwords. You may even get spam emails that appear to be from your contacts or friends.

## SOCIAL MEDIA SPAM

The rise of social media has inevitably led to the growth of social spam. Typical social spam tricks you into liking/sharing content (like-jacking), or promoting malware from a 3rd party site. Social spam can be hard to spot as the message generally comes from one of your friends and can be personalised.

## COMPUTER VIRUS SCAM

If you've been targeted by the computer virus scam and downloaded software that gives scammers access to your computer, it's a good idea to have your computer checked for spyware.

## What you can do to protect yourself?

*If an email seems unusual or suspicious don't open it – even if it is from a friend. Never reply or click on links, even to try to unsubscribe. And don't call any phone numbers listed in the email. If in doubt, it is best to delete the email straight away.*

*The same goes for clicking on website pop-up boxes and banners you do not trust. Don't click, just close.*

*If you see an online advertisement for an offer you can't resist, do an online search on the company name instead of clicking on the link. That way you can find out if the offer is legitimate without the risk of clicking on a malicious link.*

*Don't enter your personal details, including credit card and bank account information, on any website you are not certain is genuine.*

*Before you take advantage of a free offer, check it out with other internet users you trust, or do some research into the company making the offer.*

*Be wary of websites offering free games, music or video. The files they provide could be 'trojans' (which are explained above). Do some research to make sure that websites are reputable before you download anything or click on any links.*

*Install internet security software, including virus-and-spyware checkers. The makers of this security software regularly publish updates to deal with the latest risks. Keep this software up to date.*



## 2.5 Employment scam types

### PAYMENT ADMINISTRATION

You're asked to handle payments on behalf of an overseas company. You'll get a fee for every payment you handle. Little do you know that the money is a front for illegal activities. Without realising, you become a money mule and you could be prosecuted.

### GUARANTEED EMPLOYMENT/INCOME SCAMS

You're guaranteed a certain level of income or employment. To get it you have to buy something like a business plan, start-up materials or software. You may also be asked to pay money to be put on a directory to 'guarantee' your job. The only guarantee is that you'll lose your money.

### MULTI-LEVEL MARKETING

People selling through a multi-level marketing scheme get commission on the sales of those they recruit, as well as on their own sales. Some multi-

level marketing schemes, like selling Tupperware, are legitimate business models.

But some pyramid schemes try to disguise themselves as multi-level marketing schemes by tying the sale of products into the offer. The products are usually of poor quality, overpriced and hard to sell.

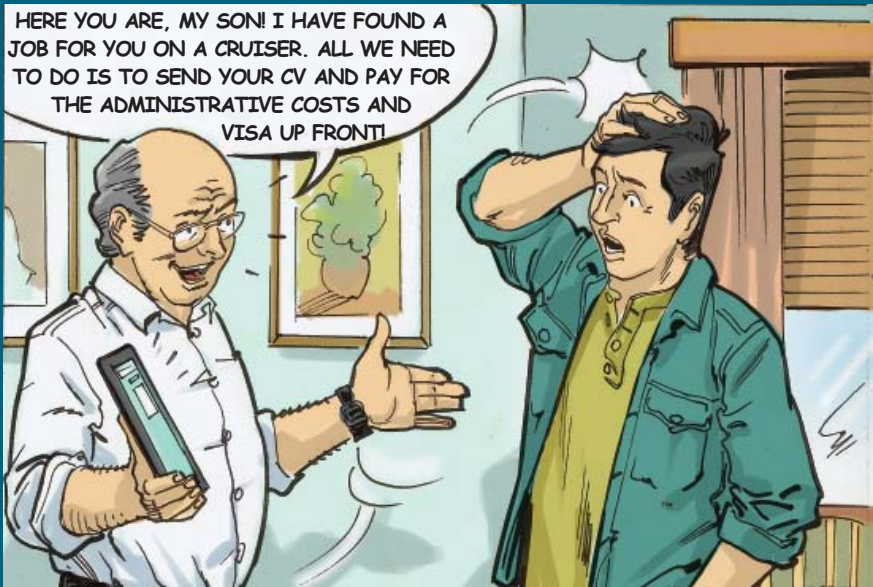
Other pyramid schemes, posing as multi-level marketing, may dupe their members into spending a great deal of money on training materials.

### SEMINARS

Scammers pose as recruitment agencies, hosting recruitment seminars. They tell you about a 'great opportunity', often overseas. At the seminar you'll be asked for upfront fees – perhaps to edit your CV, for administration costs, or for a work permit or visa. Once you've handed over the cash, the 'agent' usually disappears.

### VISA/WORK PERMITS

A prospective employer overseas says that they'll handle your work visa application. But you have to send them the money to process it. Your visa never arrives, and your 'prospective employer' disappears.



## What you can do to protect yourself?

*Look for employment through well-known recruitment websites or reputable recruitment agencies.*

*Be suspicious of online ads promoting the opportunity to work at home – many of them are scams.*

*Check out any company that offers you employment or a business opportunity. Don't be taken in by wild claims or glowing testimonials – they may not be real. Type the company name plus 'scam' into an internet search engine. You*

*may find reports from people who have been targeted by the same scam.*

*Ignore unsolicited emails. It's best to delete them without opening them. If you do open them, avoid clicking on any links, even ones that say 'unsubscribe' – they may launch spyware or viruses on your computer.*

*Check out any job offer carefully, especially if it's overseas. Enquire about visa costs and processes from the relevant visa authority. Never send money overseas unless you completely know and trust the person or organisation.*

*Contact your bank if you have received money into your bank account that you believe to be illegal.*

## 2.6 Investment scam types

### COLD CALL INVESTMENT SCAMS

This type of scam is sometimes called 'boiler room' fraud. It's usually a slick operation. A professional sounding 'broker' calls you with an offer that's hard to resist. It will probably relate to an overseas company.

They're likely to back up their claims with credible-sounding business names and genuine-looking documentation and websites. They may say that they're stock brokers or portfolio managers, approved by a trusted company.

Working from a convincing pre-prepared script, the scammer may offer you:

- shares
- mortgage 'investments'
- real estate 'investments'
- investment schemes
- option trading or
- foreign currency trading

The scammers can be very persuasive. They'll promise high, quick returns on your investment for little or no risk.

The risk, of course, is that the investment is a scam, and you'll never see your money again.

### **SHARE 'HOT TIP' SCAMS**

These scams usually start with an email from a 'company insider'. You're told that stock in a certain company is set to rise dramatically. The email may even be addressed to someone else - so that it looks like you've received it by mistake.

You check out the claim. Sure enough the stock is rising. That's because it's being ramped up by investor response to the scammers' email.

You buy. The stock price plummets because of mass selling. You lose a lot of money. The people who sent out the message, on the other hand, make great profits because they sell at the peak of the market.

Any stock can become the target of share ramping. It's easy to fall for as scammers appear to have 'inside info'. But it's unlikely that the scammers have any connection with the company whose shares are being ramped. Remember, insider trading is illegal.

### **INVESTMENT SEMINARS AND REAL ESTATE SCAMS**

Scammers sometimes use seminars on how to build wealth to target would-be investors. They create a high-pressure, act-now environment to draw people in.

Of course, there are many legitimate seminars. The key is to look at what is being offered. Don't be pressured into a decision before seeking trusted and professional independent advice.

As well as pressuring you to put money into bogus investments, scammers make money from admissions and expensive reports and consultancy that have little or no value.

These seminars can be full of deceptive and misleading statements - about fees, commissions to the salespeople, rent guarantees and discounts for prompt purchase. Make sure you test every claim.

### **PREDICTION SOFTWARE**

Computerised gambling systems promise to predict accurate results for horse races, sports events and even share markets.

While there are legitimate software packages to monitor investment variables, the scammers make exaggerated claims that you'll be able to make money through betting.

Scammers charge a lot of money for these programmes and often they will pressure you into sending more and more money. They'll tell you that your investment has lost money, but if you send just a little bit more you can get it back.

### PYRAMID SCAMS

Pyramid scams promise money, or some other reward, for recruiting new members into a pyramid scheme. You might be approached at a seminar, home meeting, over the phone or by letter or email.

You send fees to the person who recruited you. You then have to convince more people to send money to you.

But pyramid schemes only work for those at the top of the pyramid. It's a mathematical impossibility for pyramids to continue as you soon run out of potential members.



## What you can do to protect yourself?

*The safest way to invest is through a registered broker or registered financial advisor and investment products must include a registered prospectus.*

*If you agree to invest, but change your mind, don't be swayed by offers to swap your investment for a different one, or by assurances that your investment will soon rise in value.*

*Always seek independent financial advice before making any investment decisions. Don't rely on the advice of the person trying to sell you the investment.*

*Don't be pressured into make a decision quickly. A reputable broker gives clients plenty of time to consider and investigate their proposition.*

*Before signing up to any multi-level marketing scheme, question whether it could be a pyramid scam. Do the products and services impress you? Will you be able to sell them?*

## 2.7 Upfront payment scams

Asking for an upfront payment is a common trait of many scams. The scam usually works in one of two ways:

- Inviting you to unlock a large amount of money by sending an upfront fee.
- Appearing to overpay you for a transaction, product or service then asking you to send a refund, or to forward the balance on to somebody else.

### Types of upfront payment scams

#### **NIGERIAN SCAM**

It's commonly known as the 'Nigerian' scam. But it can come from anywhere in the world. It works like this:

You receive an unexpected text, email or letter.

The letter is supposedly from someone connected to a senior government official - such as a Prince, a top executive or public servant - most commonly in a West African nation such as Nigeria.

They want to use your bank account to get funds out of their country - usually huge amounts in the tens of millions of US dollars.

In return for transferring funds you're promised a large amount of money.

If you respond, you'll be asked for your bank details. You'll also be asked for some 'fees' in advance so that the transfer can be made.



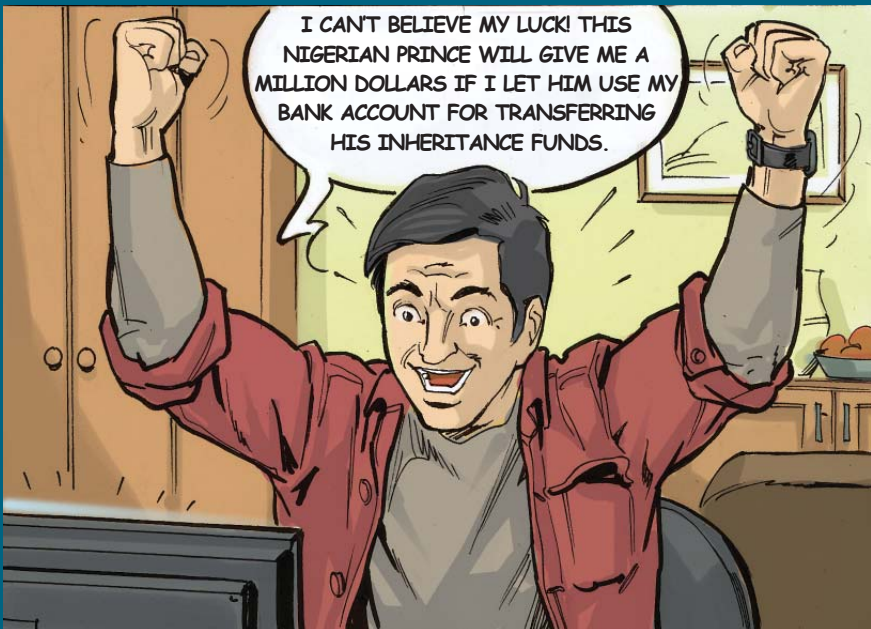
The fees can start out as small amounts, creating a false sense of security. However, the scammers know that once you've invested some money in the scam, you're much less likely to walk away. They will ask for higher and higher amounts for new fees that need to be paid before you can receive your 'reward'.

Money may be 'trapped' for dramatic-sounding reasons such as civil wars, coups or exotic natural resources. Inheritances may be 'trapped' by government restrictions or local taxes.

In essence, the scammers are asking you to launder money. Even if their claims were true, money laundering is illegal.

### **INHERITANCE/ESTATE FUNDS SCAMS**

You're approached by somebody claiming to be from an estate company. They're trying to track down the beneficiaries of a will. Apparently you're the 'next of kin'. They may refer to an event like an airline crash to make the death sound more convincing. You may check it out and find that there is a dead person who shares your last name. They want you to send legal fees in advance of receiving your inheritance. Of course there is no inheritance or long-lost relative, and the 'estate company' will disappear once they've got your funds..



## What you can do to protect yourself?

*Don't respond to an unsolicited email or letter. Never click 'unsubscribe' on a spam email: it only tells spammers that you read spam. Delete the email, or throw the letter away, immediately.*

*If you've begun to pay 'fees' to a scammer, the only way to get the scam to stop is to stop*

*paying. Once you've parted with some money, it can be tempting to see things through – just in case. But there is no reward waiting at the end of this process. You will never be paid.*

*Remember that money laundering is illegal. Never agree to transfer money for someone you do not know. Contact your bank if you have received money into your bank account that you believe to be illegal.*

## 2.8 Mobile phone scams

As people go mobile, so does cybercrime. Smartphones open new doors for cybercriminals and scammers. They are mini-computers. A gateway to billing accounts, email accounts, text messages... The list goes on.

Cybercriminals can on-sell valuable personal information. This may also use your information to steal your identity, or to target you with other scams.

Even if you don't have a smartphone, you can still be affected by a mobile phone scam.

Lost your phone? If it is not locked with a password, whoever finds it has access to all of your data. And they haven't needed to do a single thing.

Mobile phone scams work by:

- Using malicious applications to take over your smartphone
- Tricking you into texting or phoning a premium rate number and making massive charges to your phone bill

## Types of mobile phone scam

### MALICIOUS APPS

You can download an app for pretty much anything. To get you to your nearest café, to measure your heart rate, to help you redecorate your house... But not all applications are created equal. Cybercriminals use apps to hide malware that, when downloaded, gives them complete control of your phone. And, most of the time you won't even notice.

## COMPETITIONS OR QUIZ

This type of scam can affect you whether you have a smartphone, or not. You're sent a text inviting you to enter a competition or play a trivia game. 'Why not?' you think.

What you're not told is that each text you send is charged at a premium rate. And you'll probably end up paying for the messages you receive too.

Some may be real games or competition. But the prize will be worthless compared with what it costs you to take part.

Or there may be no game or competition. Scammers may simply start taking money, by making charges to your mobile phone account. It's more than likely you'll only realise once you get your phone bill or run out of credit.

## MISSED CALL OR MESSAGE SCAMS

You receive a 'missed call' message. You call back, without checking the number. It turns out that the number is a premium rate call. The return call will be very expensive. The same technique can also be used with text messages..



## What you can do to protect yourself?

*Lock your mobile device with a password.*

*Consider investing in mobile management and security software.*

*Stick to official distribution channels like iTunes when choosing apps. Check the publisher and reputation of every app you download. Also check what permissions you are agreeing to before downloading.*

*Check the numbers of text messages or missed calls. Make sure the number is a standard format. If the number is unusual in any way don't respond.*

*Before responding to any text offer, make sure you can check a full list of terms and conditions. You need to know all of the charges you could end up paying. That includes charges for ending a subscription.*

*Check that it's not a scam by calling your mobile phone company. Ask them how much it costs to call the number involved.*

*Never accept any text-based offer or take part in any competition that does not tell you how to opt out whenever you want.*

*Never give out financial or personal information by text. Your bank or any other reputable bodies you deal with will never ask for information in this way.*

## 2.9 Small business scams

Running a business can make you a target for all kinds of scams. From being billed for advertising you that didn't place, to being asked to forward a payment to a non-existent third party supplier.

When cash flow is king, you can't afford to lose out to a scammer. Be aware of these common small business scams:

### FALSE INVOICES

This kind of scam is usually linked with fake publications and domain name renewals. But small businesses have been falsely billed for other products and services. The scam works in one of two ways:

- You get a fake invoice for something that you have genuinely ordered.
- You are billed for a product or service that you didn't order, but are told that you did.

It can be really easy to pay a bill without question, especially if it's for something that you order all of the time.

In the case of a publication or a domain name, a scammer may call to confirm details of an advertising order – even though your company or organisation never made such an order.

The scammer may try to confuse you, or your staff, by referencing a real advertisement, or entry, that you have made on a genuine website or publication.

### **FAKE DIRECTORIES AND PUBLICATIONS**

Some scammers will go as far as producing small print runs of magazines, or online directories, to help sell advertising to their 'clients'.

Businesses believe that they have placed a genuine advertisement when, in actual fact, the publication is seen by no more than a handful of other victims.

You may even be offered the chance to advertise for free... 'Great!' you think. Not so great is the small print that says that there is a cost for processing and administering your listing. And, that by accepting the offer, you agree to this charge.

If you refuse to pay, the scammers may try to intimidate you with threats of legal action. These threats are usually empty. But many businesses pay out before they realise that the scammers will back down if challenged.

### **AMENDED BANK DETAILS**

You get a phone call from, what you think is, one of your regular suppliers. They're just letting you know that they've changed their bank account details.

You amend your accounting system. Next thing you know, you're paying genuine invoices, from your genuine supplier, straight into a scammer's bank account. And you only realise this when your genuine suppliers gets in touch to say that your account is in arrears.

### **FAKE CUSTOMERS/ENQUIRIES**

Some scammers pose as customers that are interested in using your services.

They may ask you if you're available to take pictures at their son's wedding, for instance.

The scammer will make multiple enquiries, usually by email. They'll ask all sorts of details. By the second or third email they'll probably seem pretty committed. So you try your best to be accommodating.

At some point the scammer will arrange to pay you – in full or a deposit. When the payment shows up, it appears that they've paid too much.

Next comes an elaborate request to forward on a portion of the money to a third party – a travel agent, or limousine-hire company, perhaps. You oblige, only to find that their first payment has been reversed.

You're left out of pocket to a customer that never was. Worse still, you have been used to launder money, which is against the law.

### **SEARCH ENGINE OPTIMISATION (SEO)**

The age of the internet has seen scammers jump onto the SEO bandwagon.

They may promise to crack complicated algorithms, to build links or to have an 'inside man' at Google.

Unless you're very familiar with technology and all its jargon, it can be very easy to be ripped off.

Be very wary of spam emails, or any other approaches that come out-of-the blue that promise to turn around your business's web ranking.

Many times what they are promising is impossible. Or, at the very least, you'll be over-charged for simple steps that you could have taken yourself.



## What you can do to protect yourself and your company?

*Limit the number of people in your business that has authority to make purchases or write orders.*

*Keep written records of all orders and purchases.*

*Reconcile all invoices against actual orders. Ask for proof of purchase and check with colleagues to make sure that you have received what you paid for.*

*If an invoice seems to reference an advertisement or directory entry you*

*genuinely made, make sure that all of the details add up. False billing scammers may use your real advertising as the basis for their fake invoices, e.g. company name, address and bank details.*

*Deal only with people and companies you know and trust.*

*If you agree to buy from a new supplier, make sure you know exactly what they are offering, at what price, quality, terms and conditions.*

*Don't accept business proposals over the phone. Ask to see offers in writing before you accept them.*

*Seek advice when making a significant purchase. Don't take the seller's word about competing products or prices.*

*Be careful to read the fine print on any offer you receive. If the print is on a fax and is blurry, request a proper copy ... but only use a non-premium telephone or fax number.*

*Check any number you call or fax at a seller's request to make sure it is not a high-charging premium number. If*

*in doubt, call your telephone service provider.*

*If you receive a letter, email or phone call from a 'supplier', asking you to update their bank details, be wary. It may be a scam. Phone your supplier to verify the request. Use a phone number from a trusted source, for example the Yellow or White Pages.*

*If you're planning on optimising your website, ask a web-savvy friend, or associate, to recommend a professional who can help.*

## 2.10 Social media scam types

### MALICIOUS LINKS

Social media is a great way to share funny videos, favourite songs and other bits of trivia. But take care. What seems like harmless fun can cause problems down the line.

Scammers use catchy headlines to trick you into clicking on, and sharing, apps and links. The sorts of apps that tell you "what your friends think of you" or "who's been visiting your Facebook page?" are classic examples.

Before downloading the app you're asked for your log-in details. You fill them in, and bingo! Scammers have a free reign on your account.

Other links can launch spyware onto your computer. Spyware gives scammers access to personal details such as log-ins and address books. Once they're in, they can target your friends with malicious links.



## **PHISHING EMAILS**

Phishing emails are another method scammers use to steal your social media identity. You'll receive an email that appears to be from the social media site. This will ask you for your log-in details. They are supposedly needed to "provide you with extra security". Some emails may even ask you for your credit card details. You'll be directed to a fake log-in page that may look very convincing.

Social media sites will never ask you for financial information in relation to security. Nor will they email you attachments or links.

## **FAKE ADVERTISING**

Exercise the same caution on social media as on other websites. Not all advertisements are for genuine offers. Not only that: clicking on some may launch spyware that give scammers a direct route into your computer.

## **ROBBERY**

You're browsing around Facebook when, suddenly, one of your friends messages you. They tell you that they're stuck in another country. They've been robbed and have lost their passport and wallet. Could you send them some cash using a money transfer service?

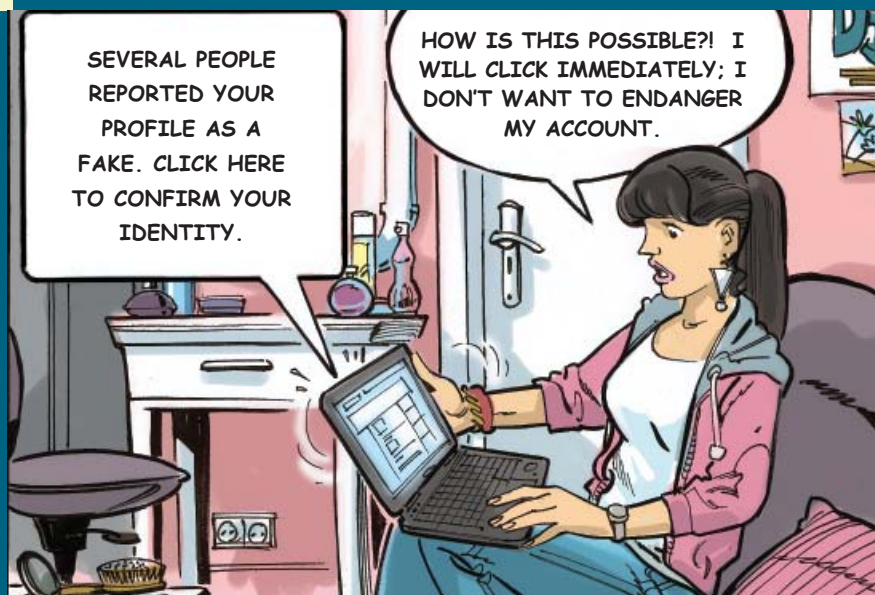
Of course you'd want to help your friend. But don't be fooled. Most of the time that this happens, it is a scammer who has stolen your friend's account and is systematically going through and contacting each of their friends to try and get money wired to them.

## **FAKE BUSINESS PROFILES**

Anyone can set up a social media page – including 'businesses'. Reputable companies use social media to connect with and keep customers up-to-date with what's going on in their business. They will never use it to ask you for money.

## **MESSAGE FROM A FRIEND**

You get a message from one of your social media friends, telling you to check out a funny video or link. Clicking on the link brings up – what you think – is the genuine social media log-in page. Entering your details gives scammers access to all of your social media friends. Not to mention the chance to download malware onto your computer.



## What you can do to protect yourself?

*Think twice before downloading applications or clicking on links to 'funny' or 'salacious' content – even if it's something one of your friends has shared. This can be tricky as social media is all about the quirky and the new. But if something seems suspicious or odd, it's best to keep aside.*

*Be wary of messages that ask you for your password, log-in and other data – even if the message points to a genuine-looking log-in page.*

*If you get a message from a friend asking you for money, ask them to call you – or to send you a number where you can call them.*


*Set your privacy setting so that only friends can view your social media content. Make sure your friends do too.*

*Think twice before accepting friend requests – how much do you really know about this person, and more importantly can you trust them?*

*Be wary of businesses or individuals that use social media as a place of trade.*



## 3. Reporting e-Crime



In today's digital world e-Crime is a fact of life and has a negative effect on the economy in general. More directly e-Crime negatively effects the competitiveness of businesses and the willingness of consumers to use digital applications to buy goods and services. It is imperative therefore that businesses, consumers and the government work together to combat e-Crime and one way of doing this is to report any e-Crime to a responsible body which will take the appropriate action to protect the community at large.

The Law on Information Security provides the basis for establishing the National Centre for the Prevention of Security Risks in ICT Systems. This centre, which is in the process of being developed, will provide valuable support to individuals, government bodies, private sector companies, agencies and others who need to be protected when being online and prevent frauds and other abuses on the Internet.

The Strategy for Information Society Development in the Republic of Serbia by 2020 defines information security as one of six priority areas of development. In addition, the National Assembly of the Republic of Serbia adopted the Law on Information Security which is designed to increase the level of information system protection and security in Serbia. It defines protective measures that are directed towards SMEs amongst others, against security challenges and threats. The Law on Information Security in defining the parameters and roles in fighting against cybercrime has led to the proposed formation of the Computer Emergency Response Team – CERT, that will provide support in ICT related incidents, raise awareness and inform the public about the need to protect ICT systems and possible risks.

Unfortunately, not all victims of internet fraud whether they be businesses or consumers receive justice, but reporting the e-crime helps in many ways. It allows the authorities to keep abreast of the cyber threats and it acts as a mechanism to warn others in order that they can protect themselves. Often those warnings are communicated in the news and result in an increase in e-crime reporting in general.

Based on the “Law on organization and jurisdiction of state authorities to combat cybercrime” the High Public Prosecutor’s Office in Belgrade processes cyber criminal cases in Serbia through a special division to combat cybercrime.

It prosecutes the perpetrators of criminal acts targeting computers (ie “every electronic device on the basis of automatic data processing and data exchange”), computer systems, computer networks, computer data, computer programs and copyright works, which can be used in electronic form.

The following provides two points of contact for reporting e-crimes and also the information that is required.

#### **REPORT INCIDENT TO:**

You should report an incident in person to Serbian police or by e-mail to:

- [vtk@beograd.vtk.jt.rs](mailto:vtk@beograd.vtk.jt.rs) (High Prosecutor’s Office for Cyber Crime)  
or
- [ukp@mup.gov.rs](mailto:ukp@mup.gov.rs) (Serbian Police – Department for Combating Organized Crime)

**SUBMIT FOLLOWING INFORMATION:**

1. Your Personal Information:
  - a. Name and Surname
  - b. JMGB (not mandatory)
  - c. Full address
  - d. E-mail address
  - e. Mobile or telephone number
2. Information about the Individual/Business that victimized you
  - a. Submit all known and / or available information
3. Monetary Loss
  - a. Specify the total amount of your loss from this incident
  - b. Did you use a third party online payment service such as PayPal or Escrow?
4. Description of the Incident and Evidence
  - a. Describe in your own words how you have been victimized
  - b. Submit all evidence you have
5. Witnesses and Victims Contact Information
  - a. If there are witnesses or other victims to this crime, provide their contact information





[www.eposlovanje.biz](http://www.eposlovanje.biz)