Identity Theft

How your business and personal finances are at risk

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

A survey by Royal & Sun Alliance revealed that British businesses regard corporate identity theft as one of the fastest growing risks they face in the future. Corporate identity theft occurs when fraudsters steal the identity of a company and then trade under a legitimate company's credit and name. It can affect companies through assets being stolen and bank accounts emptied by fraudsters trading on a company's creditworthiness, for example.

There are other threats that businesses face today that are made possible by our increasing use of technology. There is no doubt that the growth of technology has brought new opportunities to many businesses. It has changed the way in which companies do business and has opened up new information sources. But it has also created new opportunities for conmen and fraudsters to take advantage of businesses. You need to be able to recognise the threats and understand what actions you should take to avoid them.

Typical scams involve you or your staff giving away important identity information that can allow the fraudsters to use your business' credit for their own purposes.

The consequences of frauds and scams are often much more serious than the financial loss. It takes time and effort to recover from a scam, and your business' credit rating, credibility and trustworthiness may be affected for a long time.

A good way to avoid being the victim of a fraud or scam is to understand typical methods that conmen use in technology related scams. This guide explains the most common types of identity theft and other technology based threats and steps you can take to avoid them.

How to avoid Personal Identity Theft

- Shred all personal information before discarding in your rubbish; this includes anything referring to bank accounts, national insurance details, salary information, and old bank cards;
- Delete any suspicious e-mails from organisations requesting personal information from you - banks for example will not ask for such information by e-mail;
- Be extra vigilant when giving out personal information - it's easy for criminals to falsify e-mail addresses, headed paper, and other methods of communication;
- Ensure if you move house that you alert your bank and other organisations in advance so that your mail can be redirected;
- Notify the Royal Mail Customer Enquiry Line on 08457 740 740 if you suspect your mail is going missing.

Source: DirectGov

Things to look out for

You may become a victim of identity theft if:

- You have lost or had stolen important documents such as your passport or driving licence;
- Post expected from your bank has not arrived or you are receiving no post at all.

You may already be a victim of identity theft if:

- You identify entries on your personal credit file from organisations you do not normally deal with;
- Items have appeared on your bank or credit-card statements that you do not recognise;
- You applied for a state benefit but are told that you are already claiming;
- You receive bills, invoices or receipts addressed to you for goods or services you haven't asked for;
- You have been refused a financial service, such as a credit card or a loan, despite having a good credit history;
- A mobile-phone contract has been set up in your name without your knowledge;
- You have received letters from solicitors or debt collectors for debts that aren't yours;
- Financial institutions that you do not normally deal with contact you to chase an outstanding debt.

Source: Home Office

The FSB issues warning on identity fraud

The Federation of Small Businesses (FSB) has issued a warning to small business owners to take action to lower the risk of being caught up in identity fraud.

David Croucher, FSB Home Affairs Chairman, said: *"It is often assumed that identity fraud only affects individuals, but it is becoming increasingly clear that small businesses are in danger as well. The livelihoods of the owners and the jobs of 12 million employees are at risk."*

"That is why it's so important for small businesses owners to take adequate precautions, like shredding documents, protecting IT systems and checking the details of debtors. Small employers should also be very wary of anyone that makes unexpected contact by phone, fax or e-mail and asks for sensitive information about the business.

"It is so much easier to take some simple precautionary steps now than to have to try to sort out the mess later on, which can take months or even years of paper-chasing."

More information is available at the website http://www.stop-idfraud.co.uk which includes advice and a test to see how at risk your business is from identity theft.

Personal and corporate identity theft

Identity theft involves fraudsters obtaining sufficient information about a person to be able to assume their identity and obtain goods, credit or services in the false name. Identity theft is quite widespread and can cause enormous problems for both individuals and businesses. If a fraudster can get sufficient information about a business or person, they may be able to apply for a corporate credit or debit card and go on a spending spree. Such cards can be readily used in electronic transactions.

As part of your security policy, you should implement guidelines on what personal information should be divulged to third parties, particularly by electronic means such as e-mail.

Corporate identities can also be stolen. This type of identity theft can have appalling consequences for businesses. For example, it is possible to submit forms to Companies House that will:

- change the registered address of a company;
- change the company secretary or director;
- appoint new directors.

Unfortunately, Companies House do not notify the true company secretary or directors that these forms have been lodged. Neither do they check any of the details for validity.

The "new" directors can open new bank accounts, have goods delivered to the "new" address, and effectively ruin the credit rating of the business and leave it with massive charges to clear.

To avoid this form of corporate identity theft, Companies House recommends that you use the Companies House "PROOF" scheme of electronic filing. PROOF (PROtected Online Filing) enables companies signed up to the service to only file specific forms electronically.

The scheme is designed to help companies protect themselves from fraudulent filings as it prevents individuals from filing certain paper forms. The forms covered by the PROOF scheme are:

- Appointments
- Terminations
- Change of Particulars (Company Officers)
- Change of Registered Office Address
- Annual Return

In order to take advantage of the PROOF scheme, you must be a registered user with the Companies House' WebFiling or Software Filing services and provide your Company Authentication code on the 'Opt In - PR1' form. The form will not be accepted without it. For further information visit: http://www.companieshouse.co.uk/infoAndGuide/proof.shtml

How to avoid Corporate Identity Theft

- Check your company details are correct at Companies House;
- Sign up to Companies House Monitor system – an e-mail alert warning the password holder when any future changes to company details are lodged;
- Sign up to the Companies House PROtected Online Filing, or PROOF. This enables companies to only file specific forms electronically, such as appointment/termination/change of particulars of directors and a change of registered office;
- Check prospective employees' CVs and use recruitment security checks. Many scams still require an insider;
- Own all permutations of your company name so that fraudsters cannot set up a rogue website or contact your customers from e-mail address that looks legitimate, e.g. royalsun.com/royal-sunalliance.com/royalandsunalliance.com/royalsun-insurance.com. Remember to register both.com and .co.uk variations;
- Make sure that all employees have secure passwords that are not written down anywhere (e.g. on post-it notes);
- Dispose of company stationery, including letterheads and bank details, in a secure way.

Source: Royal and Sun Alliance

Corporate Identity Theft to cost businesses £700 million a year by 2020

Corporate identity theft is predicted to cost businesses £700 million a year by 2020 (an increase of 1,300% on current figures) according to the Risk Uncovered Index by leading commercial insurer Royal & Sun Alliance (R& SA).

According to the R&SA research, large businesses, with over 250 employees, will pick up the biggest share of costs from corporate identity theft and London firms are forecast to be hit by the greatest increase in costs at £140 million by 2020. The sectors most likely to be affected are communications, banking, finance and insurance.

Information requests

A fraudster may try to get you or your employees to reveal information that can be used for more serious attempts to defraud you. For example, they may phone one of your employees, pretend to be from your IT department and request the employee's password to fix a problem with their e-mail account. The fraudster can then use that password to enter part of your protected systems and do further damage. Unlikely as it may seem, this simple method can work with a large number of employees.

Phishing

Phishing is the practice of sending false unsolicited e-mail messages to a wide audience, often using spamming lists. The most common phishing e-mails are designed to look as if they come from a bank or similar organisation asking recipients to confirm their account details, including account numbers and online banking security information. They usually give a plausible reason for requesting such details - for example, to maintain or restore an account.

The e-mails often link to a webpage which has an appearance very similar to the web application page that users normally see when they log in to their account. Users are prompted to respond to the message and to supply secret information such as a name, password or credit or debit card details. The information supplied can then be used by the phisher to make purchases or extract cash from the user's account or a business.

Avoidance

The key to avoiding phishing is recognising the scam. The best approach is to ignore any e-mail message that appears to come from a bank or a similar institution asking you to connect to a website and supply information. Banks will never ask for information in this way. If you are in doubt, contact the bank at your usual branch and check if the contact is genuine.

Phishing can target your business directly as well as your employees. You need to raise awareness of the problem so that employees can recognise the scam and respond appropriately.

Spoofing

Spoofing is used to impersonate a trusted user or computer by sending a message appearing to be from that trusted source. The message may be an e-mail message, or data going straight to a server.

The Internet and the local area networks used by most businesses rely on the Internet Protocol (IP) for sending data between computers. The IP breaks data down into packets that carry labels showing where it should go and where it comes from. Spoofing involves forging the address from which the packet appears to come so it is accepted by your business as being legitimate.

E-mails can be spoofed in the same way. This allows the perpetrator to send a message that appears to come from a trusted source, perhaps yourself, which will be accepted by the recipient. The message may say derogatory things about a competitor or a customer or may cause a fraudulent order to be accepted or placed. The resulting damage could be significant.

It is possible to follow the route that an e-mail has travelled to see where it actually came from, but a sophisticated spoofer will make sure that their messages cannot be tracked in this way.

Avoidance

To ensure that people can always tell if your e-mails are genuine, use some simple encryption techniques to make it impossible to forge them. This can be done using products such as "pretty good privacy" (PGP) or those utilising the OpenPGP standards. To ensure that spoofed IP addresses are not used to attack your business systems, you can achieve a good measure of protection by using a firewall. For example, a firewall can detect an incoming packet that has a spoofed internal source address, because it knows which IP addresses belong to the internal part of the business' network – i.e. the computers that the business uses internally. If data is coming into the company from outside, with an internal source address, the firewall knows that this is a spoofed address since such data never needs to cross the firewall.

Advance fee fraud

Advance fee frauds (AFFs) often originate from certain parts of Africa. AFFs are often called 419 schemes after section 4.1.9 of the Nigerian penal code. Common characteristics of an AFF scheme include:

- An individual or business receives a communication, typically an e-mail, from an "official" purporting to represent a foreign government agency. They will often claim to be a senior civil servant;
- The fraudster offers to transfer millions of pounds into the victim's personal bank account, claiming that the funds have come from projects that have been "over-invoiced" or are excess funds from a previous political regime and cannot be accounted for;
- The "pay-off" is that the victim is offered a percentage of these funds for their trouble, often amounting to thousands or even millions of pounds;
- The perpetrator will induce a sense of urgency and stress the need for secrecy;
- Victims are often encouraged to travel to the source country to complete the transaction and are asked to pay various fees for the trip;
- Victims are nearly always asked to provide blank company letterhead, bank account information, telephone/fax numbers etc;
- Fraudsters will often send official-looking documents with seemingly authentic stamps, seals and logos;
- Sooner or later the victim will be asked to provide up-front fees for various taxes, legal costs, transaction costs or bribes.

Avoidance

If you receive a message that you suspect is an AFF scheme or variant, do not respond as this may simply prolong the correspondence. Make sure that your staff understand that they should not respond to AFF messages and add this to your IT security policy and training. A good e-mail filter will block many of these types of message. If you do not use such software then you should investigate doing so - it will help to reduce spam as well. See our guide on the benefits of e-mail and the Internet.

Fraudulent websites

A website is an ideal way of selling goods and services. It is cheap to set up and can be changed rapidly. Many businesses now use websites as their primary sales channel.

From a buyer's viewpoint, websites are also very useful. If you need a product or service, you can type your requirements in to a search engine and probably locate dozens of possible suppliers. This makes it much easier to find unusual items.

Unfortunately, both of these advantages also apply to conmen. It is simple, for example, to set up a website that can apparently provide your business with a bargain purchase, and then take your payment without sending you the goods you ordered.

Impostor sites

In another version of this scam, some fraudsters have set up websites with domain names that are very similar to those of popular sites with high sales volumes. Through these impostor sites they can gain a significant income from buyers who mistype a web address.

You cannot rely on the contact information that these sites may include such as telephone numbers, to verify that the site is valid. The telephone may be answered by the fraudster in a convincing way.

The worst of these sites are eventually detected and added to a database of such sites by the various web-filtering services. The providers of such services usually accept reports about possibly fraudulent websites.

Avoidance

You should make it a matter of corporate policy that your employees only do business through websites and addresses that are known to be reputable.

If your business does get caught by one of these scams, it may be possible to discover a little about the physical location of the website and the people behind it, but in general it is unlikely that you will recover any payments.

Telesales scams

Cold-calling is a well known telesales tactic. While many cold calls come from legitimate companies, others will use deceptive sales practices.

"Support Publishing" cases involve companies cold-calling businesses to sell advertising space in publications, such as diaries, wall-planners and websites. They claim that the advertiser is supporting a good cause, such as a charity or the emergency services. In reality, only a tiny percentage - usually less than 2% - of the advertising revenue generated is sent on to the good cause. In contrast, the operators of the Support Publishing companies enjoy large profits.

There are a number of ways to identify calls of this nature. Often, the telesales staff will claim falsely that your business has already placed an order for an advertisement or you have previously supported the good cause. They may also claim that the Support Publishing company is a charity itself.

These types of claim are normally made in the first telesales call. A second call is then usually made which "confirms" that the order has been placed and is often pitched as a "binding contract" between you and the company. Frequently, this is followed by aggressive forms of debt collection, such as numerous phone calls, letters threatening legal action or even visits by in-house collection agents.

Avoidance

To prevent your business from being taken in, it's important not to agree to advertising that you do not want or be pressurised into paying for something that you've not requested. Be prepared to ask questions which will expose deceptions. This could include asking for information about the contractual relationship between the Support Publisher and the charity involved, or details about the distribution of the publication.

To find out how to protect your business from similar scams, read about publishing and marketing scams on the Trading Standards Central website http://www.tradingstandards.gov.uk

Dealing with the consequences of scams

If you believe that your business has been the subject of a scam or fraud, you need to take action to:

- stop the fraud continuing;
- discover the extent of the damage;
- clean up the results of the fraud.

The exact course of action will depend on the nature of the fraud, and you will need to take specific advice from the police or legal advisors, but consider the following:

- Inform the police. There is a National Hi-Tech Crime Unit that may be relevant to some forms of fraud. Take guidance from the police on which, if any, of these subsequent actions should be taken;
- Check bank accounts for unexplained transactions;
- Run a credit check on your business - these are relatively inexpensive and may help to pick up unexpected changes in your business' credit condition. You can find out about credit checks at the Better Payment Practice Campaign website http://www.payontime.co.uk/collect/collect_main.html;
- Be particularly careful in making future payments - ensure that these are for goods and services you have actually received;
- If the scam involved penetrating your IT systems or you think that information from these systems might have been used, then the systems themselves may still be compromised. Unless you have particularly good internal IT security expertise, you should consider hiring an IT security specialist to investigate and, if necessary, rebuild or replace parts of your IT infrastructure.

Prevention is far better than cure. The consequences of a scam can take a lot of time to clear up and they can threaten your business' viability.

How ID Fraud occurs

- Internet Sites – Anybody that uses the internet will regularly be asked to share personal information to gain access to websites and buy goods.

  Fraudsters can combine the personal information you provide to unsecured internet sites such as your mother's maiden name with other bits of valuable information they glean about you to obtain credit in your name.

- Mail Forwarding – by completing change-of-address forms to redirect your mail fraudsters can receive a wealth of information about you delivered direct to their doorstep.

- Phishing – This term describes identity theft via e-mail. Fraudsters will send an e-mail claiming to be from a bank, Credit Card Company or other organisation, with which you might have a relationship asking for urgent information.

  Typically the e-mail will ask you to click on a link to enter your account details on the company's website to protect against fraud or to avoid your account being deactivated. But if you click on the link in the e-mail you will be taken to a website which looks genuine but has in fact been created by fraudsters to trick you into revealing your private information. The fraudsters then use the information provided to set about obtaining money from your accounts.

- Theft of Wallet or Purse – the average purse or wallet contains bank cards, credit cards and valuable identity documents including driving licenses and membership cards. Victims realise very quickly that their wallet has been stolen but often do not realise the value of the information contained within it until it is too late.

- Unsolicited Contact - Phone calls claiming to be from banks asking you to update your personal information should be regarded with caution. Calling the switchboard of the company in question and asking to be put through to the person who called you will help ensure you are not playing into the hands of fraudsters.

  Similarly, fraudsters posing as market researchers may ask for personal information over the phone. Credible organisations will not mind you double checking their authenticity before providing such information.

- Bin raiding – Fraudsters pay people to go through the rubbish you throw out, looking for bank and credit card statements, pre-approved credit offers, and tax information. Everyday information that you may not think is important such as old gas, electricity and telephone bills, insurance documents, bank statements and even personal letters and envelopes they were sent in, carry valuable personal information that can be gathered together to steal an identity.

  A 2005 bin raiding survey commissioned by Fellowes showed that an alarming 77% of household waste contained at least one or more items which could assist fraudsters in stealing an identity.

- Card skimming – This usually occurs when a shop assistant or waiter, for example, gets your information by 'skimming' or copying your credit card information when you make a purchase. They often then sell the information to professional criminal gangs. Like phishing, skimming can be used on its own to collect enough information on your credit card to use your card fraudulently without stealing your entire identity.

- Corporate Identity Theft – It is not just the individual at risk, but also companies. By accessing publicly available company records fraudsters will change names of company principals and registered addresses. They will then trade off the back of the real company's good name and obtain goods and services on credit from suppliers. This is not the only area of risk. Company bank details may be in the public arena in order to encourage customers to pay for goods directly into the company's bank account. Fraudsters will obtain signatures from the public records and attempt to attack these company bank accounts by purporting to be the signatory on the account.

- Impersonation of the Deceased – Ruthless criminals have been known to use the identities of deceased people to carry out fraudulent activity. Fraudsters will note the age, date of birth and address of deceased people from announcements relating to the death or the funeral. Alarmingly, CIFAS - The UK's Fraud Prevention Service, estimates there were over 80,000 incidences of deceased identity fraud in 2005. 'Day of the Jackal' frauds, where the deceased was aged 18 or under, are estimated to represent up to approximately 18% of the total, based on some research from 2004.

Source: www.stop-idfraud.co.uk

Identity Theft Insurance

A number of banks, insurers and other institutions now offer ID theft insurance. If your identity is stolen, the insurer will provide both administrative and financial support to manage the associated problems including lack of access to money.

Most insurers offer identity theft protection at between £4 and £8 a month if paid monthly or at a small reduction if paid annually.

Policies typically provide cover for the expenses incurred if your identity is stolen. These might include:

- legal fees resulting from identity theft related criminal charges;
- rejected loan application fees;
- emergency money if you are unable to access your bank accounts or credit cards;
- fraud liability if fraudsters apply for, and obtain credit cards, debit cards, charge cards or new bank accounts in your name;
- telephone calls and postage; and
- lost wages if you have to take time off work to reclaim your identity.

They may also include access to your credit report and will notify you if any changes are made to your report – such as a loan being taken out in your name.

If you have suspicions that you are a victim of identity theft – or have evidence to show that you are - your insurer will allocate you an identity theft expert to help you with your case. They will be able to answer any questions you have, solve issues arising due to your stolen identity and assist in correcting your credit file.

Identity theft insurance or protection is offered by a number of financial institutions including:

- HBOS group www.bankofscotlandhalifax.co.uk/SecurityandPrivacy/identitytheft.asp;
- Sainsburys Bank www.privacyguard.co.uk;
- Card Protection Plan www.cpp.co.uk;
- BT www.btidentityprotection.bt.com

Useful Links

Information about identity theft

- General identity theft information
  www.identityfraud.org.uk
  www.identitytheft.org.uk
- APACS - the UK payments association
  www.apacs.org.uk
- Bank Safe Online
  www.banksafeonline.org.uk
- British Bankers' Association
  www.bba.org.uk
- CardWatch
  www.cardwatch.org.uk
- CIFAS - The UK's Fraud Prevention Service
  www.cifas.org.uk
- Financial Services Authority
  www.fsa.gov.uk

General fraud prevention

- Antiphishing
  Read about Internet scams at:
  www.antiphishing.org
- Companies House
  Read about corporate identity theft and how to counter it at:
  www.companieshouse.gov.uk/infoAndGuide/proof.shtml
- Crimestoppers
  www.crimestoppers-uk.org
- Fellowes
  www.fellowes.co.uk
- Fraud Reduction
  www.uk-fraud.info
- Home Office
  Read Internet crime prevention advice at: www.homeoffice.gov.uk/crime-victims/reducing-crime/internet-crime/
- Identity and Passport Service
  www.ips.gov.uk
- Metropolitan Police Fraud Alert
  www.met.police.uk/fraudalert
- Telephone Preference Service
  Find out how to opt out of receiving unsolicited sales and marketing calls at:
  www.tpsonline.org.uk/tps
- Trading Standards
  Read about publishing and marketing scams at:
  www.tradingstandards.gov.uk/cgi-bin/bglitem.cgi?file=badv641-1011.txt

To get your credit file

- Callcredit plc
  www.callcredit.co.uk
- Equifax
  www.equifax.co.uk
- Experian Ltd
  www.experian.co.uk

Further Information

Age UK publish very useful guides on ID fraud and scams: for information, visit: http://www.ageuk.org.uk/money-matters/consumer-advice/scams-advice-landing/?ito=2649&itc=0&gclid=CODMr_i9hK8CFWIntAodsHx93A

This publication is for general interest - it is always essential to take advice on specific issues.

We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

Acknowledgement

[1] © Some of the information in this publication has been derived from government sources and Crown Copyright therein is duly acknowledged.

Important Notice

Publication issued or updated on: 26 March 2012

Ref: 586