



IDENTITY THEFT

STAY SAFE ONLINE: PROXIMAL CONSULTING'S INTERNET SECURITY TIPS

"SCAM BAITERS" TAKE REVENGE ON 419 FRAUDSTERS

FOCUS ON FRAUD: ONLINE DATING SCAMS

SERVICE DIRECTORY & CONTACT DETAILS

■ In this edition of the Proximal Consulting Review we bring you an online crime special looking at the threats involved, as well as ways to stay safe online and protect your identity. We also feature articles on Internet dating and the increasingly popular "sport" of scam baiting. As always, we look forward to receiving your comments - you can contact us at newsletter@proximalconsulting.com.

IDENTITY THEFT

■ Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime such as fraud or theft. Identity thieves steal key pieces of personal information – either physically or in other ways, without your knowledge – and use it to impersonate you and commit crimes in your name. Identity thieves can manipulate your information and invade your personal and financial life. They can use stolen identities to conduct spending sprees, open new bank accounts, divert mail, apply for loans, credit cards and social benefits, rent property and even commit more serious crimes. If your identity is stolen, you can have difficulty getting loans, credit cards or a mortgage until the matter is sorted out.

10,000
British passports were issued to fraudulent applicants between 2005 and 2006



personal details such as name, home address, e-mail address and even height and eye colour with the fake companies. Some scammers have apparently gone as far as to hold mock interviews to add realism to their scams.

- Also in March 2007, it was reported that hackers had stolen information from at least 45.7 million payment cards used by customers of the US retailer TJX, which owns TJMaxx and the UK outlet TKMaxx. The full extent of the theft and its effect on customers is not yet known.

Identity theft costs the UK economy approximately **£1.7 billion a year**

IDENTITY THIEVES MAY OBTAIN YOUR PERSONAL INFORMATION BY:

- Removing mail from your mailbox or fraudulently redirecting your mail.
- Stealing personal and private information from wallets, purses, mail, your home, vehicles, computers, and websites you've visited or e-mails you've sent.
- Retrieving personal information in your garbage or recycling bin by "dumpster diving".
- Posing as a creditor, landlord or employer to get a copy of your credit report or access to your personal information from other confidential sources.
- Tampering with ATMs and point of sale terminals, enabling thieves to read your debit or credit card number and PIN.
- Searching public sources such as newspapers (obituaries), telephone books, and records open to the public. Online access to many of these information sources has made this method much easier for thieves today.
- Buying the information from a dishonest employee working where personal and/or financial information is stored.

The average Briton is a tantalizing **£85,000** target for identity fraudsters

SOME OF THE BEST THINGS YOU CAN DO TO PROTECT YOURSELF ARE SIMPLE COMMON SENSE - HERE ARE OUR TOP TIPS:

- Never give personal/account details to anyone who contacts you. No bank or building society would EVER contact you for your PIN or password, so never disclose this information.
- Keep any passwords and PINs secure – never write down your PIN or keep it with your card and don't use the same password for more than one account.
- Check your statements as soon as they arrive and immediately contact the bank if any unfamiliar transactions are listed.
- If you move, or have your mail redirected, ensure you give your new address to your bank, credit card company and anyone else you deal with.
- Cancel any lost or stolen credit or debit cards immediately.
- When using your credit or debit card make sure other people can't overhear you or see your personal information.
- Keep your personal documents in a safe and secure place at all times.
- If you lose your passport or driving licence, or have it stolen, immediately contact the organisation that issued it.
- Destroy bills, receipts, credit or debit card slips, bank statements and unwanted post, preferably by using a shredder.
- Regularly get a copy of your personal credit file from a credit reference agency such as Experian or Equifax to see if it includes any entries you don't recognize.

IDENTITY THEFT IN THE NEWS:

- In October 2006 it was reported that criminal gangs had infiltrated ten percent of Glasgow's financial call centres, stealing customers' identities either by placing gang members in call centres or by intimidating employees to provide sensitive customer details. The information was then used to steal identities and fraudulently set up accounts or transfer money. It was estimated that the sums of money stolen ranged from a few thousand to over one hundred thousand pounds.
- In March 2007 job hunters were warned to be careful when using online job sites to find employment. Fraudsters have reportedly been sending bogus e-mails to job hunters purporting to be from genuine companies offering "fantastic opportunities". Victims are enticed to "register"

STAY SAFE ONLINE: PROXIMAL CONSULTING'S INTERNET SECURITY TIPS

■ A recent government-backed survey found that people in the United Kingdom feel more at risk from Internet crime than from burglary. Here we look at some of the online crime threats affecting Internet users, as well as ways to stay safe online.

“12% of UK Internet users have been a victim of online fraud in the past year”

PHISHING

Phishing is a practice in which criminals lead Internet users to counterfeit websites in the hope that they will disclose confidential information about themselves (personal details, passwords, debit or credit card numbers). The bogus websites favoured by these criminals range from banks and credit card companies to online shops and auction sites, and are usually accessed via a link embedded in an e-mail sent to the victim purportedly from a legitimate organization. Some of the fake websites and e-mails are so realistic that it can be very hard to spot “phishing” e-mails.

TOP TIPS

Common warning signs that an e-mail is bogus include:

- The sender's e-mail address or the website link do not correlate with those of the organization they claim to be from.
- The e-mail is marked 'urgent' or is unexpected.
- The e-mail contains a non-specific greeting like 'Dear Customer' or the entire text is contained within an image.

“Online banking fraud rose 44% last year to £33.5 million”

ONLINE SHOPPING

Last year 1.7 million UK Internet users fell victim to fraud whilst shopping online. Online shoppers expose themselves to a number of potential crimes or scams, from bogus online auctions to misuse of credit or debit card details. The pitfalls of purchasing goods from online retailers or auction sites include paying for goods which are never delivered, goods purchased failing to match the advertised description, or being unable to contact sellers after the transaction has taken place. Online sellers may also face problems from fraudulent customers, and should take necessary precautions to validate the credit status and delivery addresses of new clients. Online shoppers also face the risk of identity theft or credit card fraud with website security lapses exposing their credit card or personal details to fraudsters.

TOP TIPS

- When shopping online, always choose reputable sellers and remember that if a deal looks too good to be true, it probably is.
- Ensure that you are using a secure website when entering credit or debit card information; secure websites will display a padlock symbol in the lower right of the browser window and the website address will begin 'https://'.

“Online sales are predicted to top £42 billion in 2007”

SPYWARE

Spyware is an unwanted program which runs on your computer, usually having installed itself alongside another program. At best it is an annoyance, and at worst a threat to personal and financial privacy. One type of spyware, adware, can cause your computer to allow unwanted pop-up adverts (often for offensive websites), or to download adverts from the Internet to your computer. Adware can also hijack your computer changing the default homepage or putting new icons on the desktop. Sophisticated versions of adware can block anti-virus and anti-spyware defences and track your online activities in order to send you more adverts. Surveillance spyware is even more sinister. It can obtain private data (such as credit card numbers) from your hard disk, log your keystrokes thus recording passwords and credit card numbers, and capture personal information by taking screen shots of sites visited. Having obtained valuable personal and financial information, the spyware program can upload this information to criminals over the Internet. The whole point of spyware is that it operates without the computer user being aware of its existence.

TOP TIPS

- When purchasing software, always try to buy from trusted companies. Be on your guard when downloading 'free' programs or software, or peer-to-peer file sharing applications.
- Certain websites can also install spyware; be very careful before visiting suspicious websites.
- Some spyware will actually advertise 'spyware-removal programs' – this is a con. Use reputable anti-spyware software.

“46% of UK Internet users do not have anti-spyware software “

ONLINE PAYMENT SYSTEMS

Thanks to demand from online merchants and individuals, new online payment systems are developing all the time. Online payment systems enable individuals, who may not have a bank account or credit card, to shop and pay bills online, and make international person to person electronic fund transfers. Due to the anonymous nature of the system and the varying terms of service providers, these systems are open to abuse in a number of ways: not only are they favoured by the perpetrators of fraudulent online investment scams, but payment systems which accept cash and money orders can be used for money laundering and other illegal activities. As online payment systems often operate internationally, involving numerous jurisdictions, regulation and legal action can be difficult.

TOP TIPS

- Beware using online payment systems with no buyer or seller protection in place. Choose a well-known service provider and ensure that the website is secure.
- Never transfer money on behalf of someone else and only send money to people you know or whose identity you can verify – there are numerous reports of scams involving money transfer systems.
- If you operate an online payment system, make sure that you have a “know your customer” policy in place to verify that your customers are legitimate and your services are not being abused. For more information see:

PROXIMAL CONSULTING WHITE PAPER 2: PROCEDURES & CONTROLS TO STOP MONEY LAUNDERING.

“SCAM BAITERS” TAKE REVENGE ON 419 FRAUDSTERS

■ Following on from last issue’s Focus on 419 Fraud, this time we take a look at what has been described as the Internet’s first “blood sport” – scam baiting. Scam baiting is the strange Internet pastime of feigning interest in fraudulent schemes in order to manipulate fraudsters. By replying to scam “419” e-mails, the scam baiters’ principal aim is to waste fraudsters’ time, often humiliating them in the process. Some scam baiters however simply try to obtain a confession or confidential details from the fraudster, in order to pass the information on to law enforcement authorities.



There are a number of websites dedicated to scam baiting, where scam baiters can post records of their correspondence with fraudsters. The extent to which the fraudsters will go in the hope of obtaining money from the scam baiters is hard to believe, but the (sometimes extensive) e-mail correspondence between the scam baiters and fraudsters which leads to these acts is even more absurd. Scam baiters’ e-mails often become increasingly implausible as the correspondence continues. It is common for scam baiters to use pseudonyms for comic effect and to encourage fraudsters to commit strange and/or comical acts in bizarre scenarios. Scam baiters usually require these acts to be photographed, or even videoed. The “evidence” is then posted on scam baiting websites for online readers’ amusement. Listed below are a few examples of the results of scam baiting:

- Fraudsters are often asked to photograph themselves in odd situations or holding amusing (and often obscene) signs. These include photographs of fraudsters holding bread and fish, or with rocks and bricks on their heads.
- A scam baiter posing as a world famous stuntman managed to get a fraudster to send an audition video of stunts such as jumping off a roof, setting fire to his ankles, and jumping through a flaming hoop! This footage is now on youtube.com.
- In a series of increasingly bizarre e-mails, using the names of various members of 1970s television comedy sketch show Monty Python’s Flying Circus, a fraudster was persuaded to re-enact and film the famous “dead parrot” comedy sketch, under the pretext that the scam baiter was a Hollywood producer. This is also on youtube.com.

Whilst scam baiting raises a number of ethical questions, (scam baiters are arguably just as deceptive as fraudsters), scam baiters maintain that by wasting the fraudsters’ time, they are preventing vulnerable individuals from becoming victims of 419 fraud. Whether you agree with scam baiting or not, scam baiting websites do make very entertaining reading. If you are interested in finding out more about scam baiting, take a look at the following websites:

- www.419eater.com
- www.scambuster419.co.uk
- www.419baiter.com

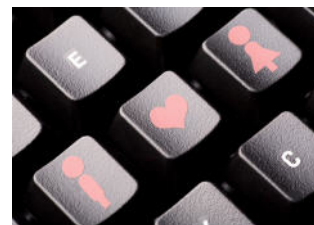
ONLINE DATING SCAMS

■ Today more and more people are turning to the Internet to make new friends and even to find love. As a result of this change in our social culture, there has been a significant rise in the number of people targeted by online dating scams designed to break hearts and steal money.



Online dating scammers, male or female, sign up to online dating agencies or chat rooms, then create false profiles to match the specification of their target victim or victims. These unscrupulous people take advantage of the anonymity of the Internet – remember many websites allow anyone to join free and they usually do not screen their members. Contact with the victim is initially made via chat rooms and e-mails and confidence is built with promises of romantic intentions. However, the scammer is only interested in one thing – money. Some of the most common reasons given by online dating scammers for needing your financial help include:

- They would really like to meet you, but don’t have enough money to travel.
- They are stranded abroad and don’t have money for travel or visa costs.
- They have been robbed and beaten and require urgent surgery or treatment for a serious illness.
- A family member has been the victim of a serious or fatal accident and you are the only person who can help them.



The scammer will ask that the money be sent to them using a method that will make it difficult to trace the ultimate end destination of the funds. Other tell-tale signs to watch out for when making friends online are:

- Your new beloved looks like a model – this is probably because he or she is using a photo of a real model from a magazine.
- Your date only gives you a post office address and/or a telephone number which he or she never answers and which does not have voicemail.
- Your new friend talks a lot about herself or himself and does not answer your questions – probably because they are sending standard e-mails to hundreds of people.

The Office of Fair Trading estimates that UK consumers lose an estimated £3.5 billion per year to a variety of scams which exploit low-cost, mass-marketing techniques. Many of these scams originate overseas, making detection and prosecution more difficult.

To avoid falling for an online dating scam, remember these simple tips:

- Be sceptical and ask yourself: “Why am I the only person who can help them when I have only just met them?”
- Always try to meet someone who lives locally. Make use of reputable online dating or chat services which match you to someone who lives closest to your post-code address.
- Never give out any personal details such as your home address or bank account and never send money to someone you don’t know.

SERVICE DIRECTORY



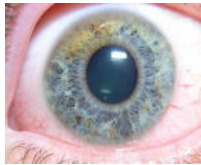
NEWSLETTER INFORMATION

Can you afford to be without this critical intelligence? You can subscribe to this newsletter and download all previous issues from our website. *Issue 3 of the Proximal Consulting Review is brought to you by Peter Lilley, Jane Smith, Alison Keyzor, James Lilley & Jo Mason.*



DUE DILIGENCE BACKGROUND REPORTS

One of our core business areas is providing global due diligence background reports on individuals and/or companies that are structured to provide focused intelligence in a cost efficient manner and in accordance with your needs. More importantly, our many years of experience in this field ensure that the legal and regulatory obligations of our clients in regard to due diligence are met. We ensure that you, as our client, are not exposed to reputational, operational, legal or concentration risks. Additionally, we have a wealth of experience in providing **MERCHANT BACKGROUND CHECKS**.



KYC DUE DILIGENCE WARNING BULLETIN

We publish a monthly KYC Due Diligence Warning Bulletin which details critical intelligence on a worldwide basis concerning individuals and companies that are known to be involved in fraudulent and/or money laundering activity. The annual subscription is £250 and includes a monthly updated fully searchable database that incorporates all entries from the first bulletin, published in February 2003. This database now contains over 5,000 warning entries.



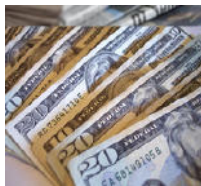
COUNTRY REPORTS

Our country reports provide you with reliable and credible advice on country risks, a further invaluable tool for staying ahead in the fast-moving international business environment of today. We analyse national and local risks in each country and provide a detailed examination of political, general business, money laundering and corruption factors.



AML TRAINING

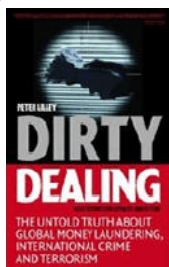
We provide a full range of high quality Anti Money Laundering training and prevention services. These include: creating and devising KYC and AML procedures, designing and delivering customised AML training packages, producing definitive AML training material (including client-specific training films), evaluating your AML "defences" to ensure regulatory compliance together with providing ongoing AML advice and guidance either on a general level or relating to specific events.



ASSET TRACING & OTHER INVESTIGATIONS

We are able to provide our clients with proven methodologies and the latest tools for investigation, evidence gathering and asset location to freeze and seize funds. Our in-house abilities together with our global network of contacts ensure that we are able to provide a worldwide coverage. Additionally, we have substantial experience in developing overall winning strategies in asset tracing projects and other types of complex and high profile investigations.

FURTHER READING...



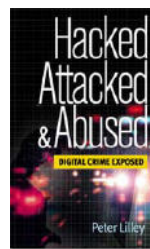
DIRTY DEALING

The third completely revised edition of Peter Lilley's acclaimed book on money laundering was published during 2006.

One of "Director" magazine's business books of the year.

"Entertaining, well written & well presented"
The Irish Times

www.dirtydealing.net



HACKED ATTACKED & ABUSED

"Hacked, Attacked & Abused" exposes the full extent of digital crime and how to avoid falling victim to it.

"This book is an excellent exposé of digital crime stemming from Peter Lilley's own expertise in the field of prevention, detection and investigation of global business crime and money laundering"

-*Asian Voice*

CONTACT US

UK Office

2 Pelham Court
London Road
Marlborough
Wiltshire
SN8 2AG
United Kingdom

Telephone: +44 1672 516725
Fax: +44 1672 516759
E-mail: enq@proximalconsulting.com
Website: www.proximalconsulting.com

Swiss Office

Rue du Rhone 14
1204 Geneva
Switzerland