Colin's Blog Special Edition

MARKING SCAM AWARENESS MONTH JUNE 2018

I Have received two emails from readers this week relating to current scams: -

"We have just had a telephone from someone saying that he was a Police Officer and our Credit Card has been used fraudulently He knew our names. He was talking to my husband at first and I was aware the call was not quite right and was trying to tell my husband not to divulge information but put the telephone down. So my husband passed the telephone to me and I said we do not wish to continue this conversation. He then tried to grip my attention saying but Madam...from which I cut the call off. I then dialled 1572 they said it was a withheld number which I could put in my junk mail box, which I did."

" I received two calls saying that HMRC is filing a law suit against me. When I did 1471 I was surprised that a number was given as I expected to hear it had been withheld. It was 0161 850 5599. I know that my tax affairs are in order but the message could scare people into phoning back. I feel I should tell someone - so I'm telling you and hope you can pass this on to whoever should know."

I thought that this is as good a time as any, to reprint my **'INTER CRIME'** articles, which serve as a reminder to all of us to think before we give out our personal information. Remember: Keep Alert, Keep Secure and Keep Safe!

Fraudsters taking advantage of the HMRC tax refund process Reprinted from a recent blog

HM Revenue and Customs (HMRC) are currently processing tax refunds after the end of the tax year and criminals are taking advantage by sending out phishing emails and text messages.

The fraudulent emails and texts include links which take victims to fake websites where their personal and financial information can be stolen.

In March 2018, HMRC requested 2,672 phishing websites be taken down and received 84,549 phishing reports. HMRC have warned that this kind of phishing is expected to continue in the coming months as genuine tax refunds are issued.

Tax refunds only come through the post or your employer

Treasury Minister, Mel Stride MP, the Financial Secretary to the Treasury said: "HMRC only informs you about tax refunds through the post or through your pay via

your employer. All emails, text messages, or voicemail messages saying you have a tax refund are a scam. Do not click on any links in these messages and forward them to HMRC's phishing email address and phone number.

"We know that criminals will try and use events like the end of the financial year, the self-assessment deadline, and the issuing of tax refunds to target the public and attempt to get them to reveal their personal data. It is important to be alert to the danger."

Other types of HMRC scams

Fraudsters also use spoofed calls and leave victims automated voicemails saying that they owe HMRC unpaid taxes.

In most cases they ask for payment in iTunes gift card voucher codes and tell victims they have arrest warrants, outstanding debts or unpaid taxes in their name.

How to protect yourself

Recognise the signs - genuine organisations like banks and HMRC will never contact you out of the blue to ask for your PIN, password or bank details.

Stay safe - don't give out private information, reply to text messages, download attachments or click on links in emails you weren't expecting.

Every Report Matters – report phishing emails to us and forward them onto HMRC at phishing@hmrc.gsi.gov.uk.

INTERCRIME ON THE INTERNET

"I don't know why you're so wary. There aren't any crooks on the Internet."

INTERCRIME 1

Phishing is the name given to the practice of sending emails at random, purporting to come from a genuine company such as a bank, but increasingly other organisations such as HMRC, in an attempt to trick customers of the company or organisation into disclosing information at a bogus website operated by the fraudsters.

Fraudsters send out thousands, possibly millions, of spam emails in an attempt to convince unsuspecting people to click onto a link that will send them to a fake sight.

These emails normally claim that it is necessary to ‘update’ or ‘verify’ your password, and they urge you to click on a link from the email that takes you to the bogus bank site.

Any information entered on the bogus website or form, will be captured by the criminals for their own fraudulent purposes.

What should I do if I have been sent a phishing email?

Any unsolicited emails should always be approached with caution, and you are advised not to follow any links contained in the email. Under the circumstances **NEVER** give out any personal details. http://www.actionfraud.police.uk/report_fraud

ActionFraud
Report Fraud & Internet Crime
0300 123 2040

INTERCRIME 2

“Wow! I just won a big prize on the Internet and all I had to do was download something that made my computer freeze up!”

MALWARE (Malicious Software)

Malware is still a very popular method used by fraudsters to obtain customers details, and is sometimes used in combination with phishing emails.

Malware includes computer viruses that can be installed on a computer without the user’s knowledge, typically by clicking on a link in an unsolicited email, or by downloading infected software.

Malware is capable of inserting bogus web pages, logging keystrokes and performing unauthorised actions on your computer, in an attempt to capture passwords, financial information and other personal details.

Make sure that your computer has up-to-date anti-virus software and a firewall installed. Consider using browser security software. Download the latest security updates, known as patches, for your browser and for your computer’s operating system (e.g. Microsoft Windows).

KEEP ALERT KEEP SECURE KEEP SAFE

DON’T BECOME A TARGET

INTERCRIME 3

Good advice from: GET SAFE ONLINE WEBSITE: https://www.getsafeonline.org

Passwords & Securing Your Accounts

Passwords are like keys to your personal home online. You should do everything you can prevent people from gaining access to your password. You can also further secure your accounts by using additional authentication methods.

Passwords: When creating a password, make sure it is long and strong, with a minimum of eight characters and a mix of upper and lowercase letters, numbers and symbols.

You should also remember not to share your password with others. Make your password unique to your life and not something that is easily guessed. It is a good idea to have a different password for each online account.

Write down your password and store it in a safe place away from your computer and change your password several times a year.

Other Ways to Secure an Account: Typing a username and password into a website isn't the only way to identify yourself on the web services you use.

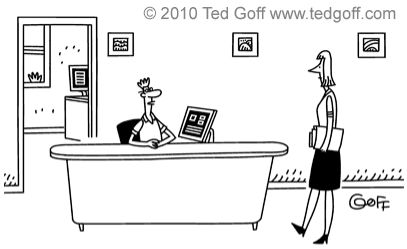
- **Multi-factor authentication** uses more than one form of authentication to verify an identity. Some examples are: voice ID, facial recognition, iris recognition and finger scanning.
- **Two-factor authentication** uses a username and password and another form of identification, often times a security code.

Over time, more websites will be adopting multi-factor authentication. In some cases, the services may be available, but are not required. Many email services offer two-step verification on an opt-in basis. Ask your financial institution and other online services if they offer multi-factor authentication or additional ways to verify your identity. **BULLET POINTS: -**

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **REMEMBER to write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.

INTERCRIME & DATACRIME 4 Follows: -



"A man who said he was here to upgrade our data spent all morning on your computer, but then left out the window when he saw you coming. Isn't that odd?"

How to get really 'hacked off!' Computer hacking is illegal and carries a possible sanction of imprisonment. Computer hacking has been thrown into the public eye recently with increasing allegations that certain newspapers hired private investigators to hack into people's phones and computers in order to obtain stories that would sell.

Computer Misuse Act

Under the Computer Misuse Act it is an offence to hack into somebody else's computer or send them a form of virus that allows them to obtain information from somebody else's computer.

The reasoning for the introduction of this Act was the fear that individuals, in particular private investigators, might be able to obtain information about other individuals without their knowledge or consent.

An individual should be entitled to keep what they have on their computer private and only allow others to use it by giving their consent, and companies have the need to store confidential data or intellectual property rights securely.

In most cases computer hacking will carry a relatively lengthy punishment because there are other more serious elements to the crime than simply computer hacking. Computer hacking is often used as a method to commit crimes such as fraud or theft. Naturally, if somebody were to hack computers to steal things from another computer then the more serious offence would be the actual theft. Computer hacking would be the aggravating factor that would add to the criminal punishment dished out by a judge.

Targets of computer hacking

A common target for computer hackers is the intellectual property of a particular individual or company. Intellectual property is a form of original creation which has the protection of a patent or copyright. But if another individual or company can claim to have come up with the product without copying the original they may well be able to sell it legally.

Computer hackers thus often target places where secrets about intellectual property can be stored and then try to remove the information from that computer. This is not only a criminal offence but also it can have serious implications in civil law if a company decides to sue the hacker for any loss as a result of the hacking.

Cyber attacks

An increasing concern to all governments around the word is the role of what is known as cyber-attacks. Cyber attacks occur when an individual or group of individuals hack into the computer system of a company, association or even government department and attempts to paralyse the system.

The motivation for carrying out a cyber attack can be vast; groups can range from those seeking information to sell on, to interest groups looking to bring down whole companies, and even terrorist groups looking to paralyse government departments.

It is on account of the vast increases in cyber attacks in recent years that government spending has increased dramatically in a bid to protect national security information. Large companies have also increased their spending on computer protection systems as often the information they hold on their computers about their products or customers is the most valuable asset of their company.

Computer hacking is illegal and carries severe penalties; it has increased dramatically over the last ten years and increasingly more groups, whether companies, governments, or even individuals are having to spend more money on computer defence systems as a result.

SOURCE: FINDLAW UK The UK's biggest online legal information site, providing daily news, blogs, forums and articles to help you understand the law. FindLaw.co.uk is part of FindLaw.com, the world's leading provider of online legal information.

"If I can't interest you in my new software, perhaps you'd like to buy the identities of the people who did buy my new software?"

INTERCRIME & DATA CRIME 5

IDENTITY THEFT – A GROWING PROBLEM

Sadly there are lots of unscrupulous people out there, just waiting for opportunities to steal your identity. Customer and Contact lists held by legitimate companies and kept on databases, are sometimes hacked into by criminals, who can then have a field day at your expense, selling on your personal details to criminals and criminal organisations.

As well as the above, there are many ways by which criminals can obtain and use your identity, so here are a few tips to help you protect your identity and prevent criminals from committing fraud in your name:-

Always keep important personal documents, plastic cards and chequebooks in a safe and secure place.

Don't share personal information unless you are confident that you know who you are dealing with.

When you dispose of statements, receipts and other documents which contain information relating to your financial affairs, **DESTROY THEM**, preferably by shredding.

Always thoroughly check bank and card statements as soon as they arrive. If you find an unfamiliar transaction, contact your Card Company or bank immediately.

Remember that your post is valuable information to an identity thief or other criminal. If you fail to receive a card statement, bank statement, utility bill or other financial information contact the supplier a.s.a.p.

If you move house, make sure that you get your mail redirected to your new address immediately.

Always make sure that you are aware of your security settings when using the internet, especially when using social media sites. Or social media.

Never share your personal data (such as your date of birth or full address on social networking sites.

It is also foolhardy, to announce information on such sites, telling everyone as when and where you are going away on holiday. If you must, it is far better, and indeed safer, to write or talk about it once you have returned. Criminals, especially burglars, relish the opportunity to glean information about you from social media and networking sites.

Putting aside the good advantages of social media. I have long been concerned about the side effects of social media sites, they play a big role in facilitating the

spread of cyberbullying. Too many people also use them to aggravate situations and to wash their dirty washing in public! An old saying with much relevance in today's world.

Check out: http://www.internetmatters.org/technologies/social-networking.html

http://www.bullying.co.uk/cyberbullying/

Did you know that according to a report by Symantec, the internationally renowned security software firm, five out of six large companies globally, were targeted by cybercriminals in 2014, with our UK companies being amongst those most frequently targeted. Apparently around two thirds of all internet-based attacks affected our small to medium sized businesses. Email remains the most popular method of attack.

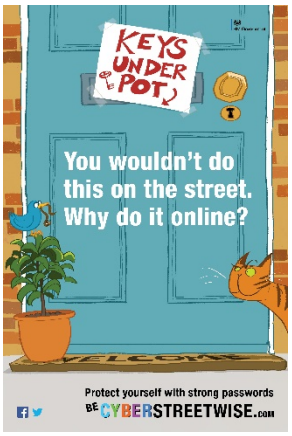
INTERCRIME & DATACRIME 6

Your password is specific and personal to you. If you give it to anyone else, it is you who will be liable, if it is used inappropriately by anyone in your organisation, to gain access to information / data held on a computer or any other device. **You** may be deemed to be in contravention of data protection law and any other related legislation.

If a colleague, supervisor, line manager, manager or director requests or demands that you tell them your password, they could also be in contravention of the data protection legislation.

Each year millions of people in the UK fall prey to scammers. Some estimates of the total cost of mass-marketed scams are as high as £5 billion. The truth is - with reporting levels as low as 5 per cent - this cost could be far higher.

However, talking of thousands, millions or even billions of pounds undervalues the wider social cost of scams: the blight they bring to people's lives, the emotional trauma for families and the loss of confidence among not only their victims, but every consumer who hears about them.



ActionFraud
Report Fraud & Internet Crime
0300 123 2040

Essex CRIMESTOPPERS
0800 555 111
Call anonymously with information about crime

CALL YOUR LOCAL POLICE
101
IN AN EMERGENCY ALWAYS CALL 999

Well, that's a large amount of information to absorb this month, but I hope it serves as a useful reminder to us all, that we are living in a technological age, which has many advantages, but, comes with the added risk of increased opportunities for those who prey on us, in their quest for our personal data to use for their unlawful gain **DON'T BE FOOLED!**

BACK TO NATURE

I hope that everyone is enjoying our current spell of good weather. I have been writing my blog, whilst listening to, or should I say, being serenaded by, my resident Blackbird, against a background chorus of many other chirping and singing birds, which bring a sense of joy and happiness to my day.

I am fortunate to have a lovely garden which, has a wonderful display of flowers, welcoming in the 'Summer weather,' and encouraging bees and butterflies, to dance around, from flower to flower in their quest for pollen. As an added bonus, my wild strawberry plants, have the best ever crop of sweet alpine strawberries this year, for me to enjoy, and giving me moments of a little nostalgia, from my childhood days.
All of these facts, help to focus my mind on the good things in life, and, indeed, for a short while, the troubles of the world, seem a galaxy way!

Mind you, having celebrated several family birthdays, and my wedding anniversary recently, I am struggling to maintain return to my diet, and the word 'Galaxy,' reminds me of chocolate. (Other brands are available) Sweet memories don't always help!

DATA PROTECTION My blog is sent to members and supporters of Epping Forest, Brentwood and Harlow NhW groups. and partnership organisations. When you join neighbourhood Watch, you agree that your contact details are shared between Neighbourhood Watched and Essex Police under existing partnership agreements, and that they are not shared with other organisations or individuals.
To unsubscribe from my blog, or from Neighbourhood Watch, please send an email to: - colin@neighbourhoodmatters.org.uk quoting the area in which you reside, so that, I know from which to list remove your contact details. Thank you.
Colin I. Freeman MITOL Trustee and Executive committee member of Essex County NhW Association, member of Epping Forest, Brentwood and Harlow NhW committees and Advisor to London Community Watch.
colin@neighbourhoodmatters.org.uk
You can also read my blog at: http://www.eppingforestnhw.org.uk/