



**FALCON**  
FRAUD AND LINKED CRIME ONLINE

# Scams, Fraud and Cyber Crime

PC Tom Lee

See here the Take five to stop fraud video: [YouTube](#)

More information on the [Take five website](#).

## Elderly 'under siege' from fake HMRC and police scammers

By Jenny Rees  
BBC Wales home affairs correspondent

### **FRAUD HELL** Student lost £17,000 life savings after scammers pretended to be from NatWest – and only got £20 back

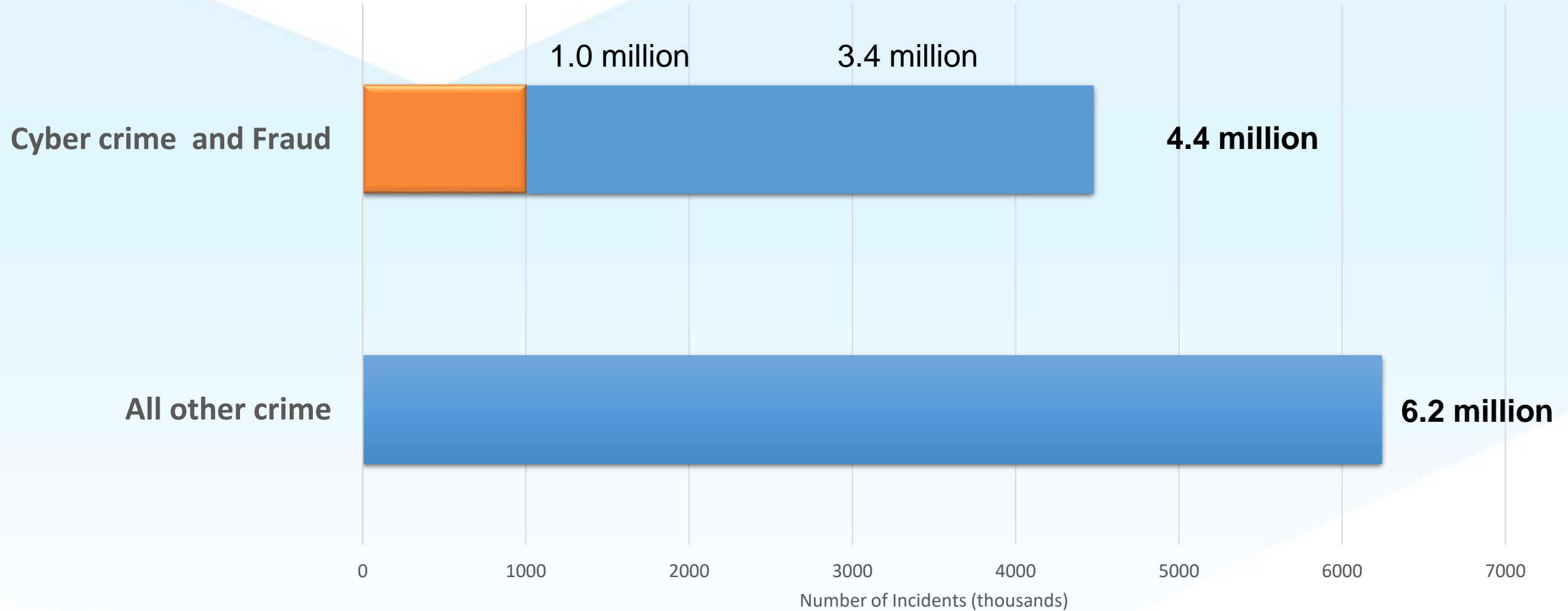
James McKendry, 27, from Oxford, has lost £17,000 after scammers emptied both his NatWest and Santander accounts of his life savings

### Police officer lost £15,000 saved up for stamp duty

Simon and Elizabeth Ghali lost £15,200 to scammers just last week.

The Ghalis, from Wakefield, West Yorkshire, are due to move house in two weeks and had earmarked part of the money to pay their stamp duty bill.





UK residents are **20** times more likely to be defrauded at their computer than held up in the street.

(NCSC, October 2017).



Over 65s are three times more likely to lose money to fraudsters than to be burgled.



(Centre for Counter Fraud Studies, June 2018).

# Fraud & cyber crime in Kensington & Chelsea



- In 2018 there were 1351 reports of Fraud & Cyber crime made to Action Fraud

£ 00,000,000

- This an average of £10,186 per victim

National Fraud Intelligence Bureau: NFIB Victim data Jan 2018 to Dec 2018



**SCAM  
ALERT**

**Fraud can be  
countered  
through  
awareness.**



# Fraud & cyber crime in the UK

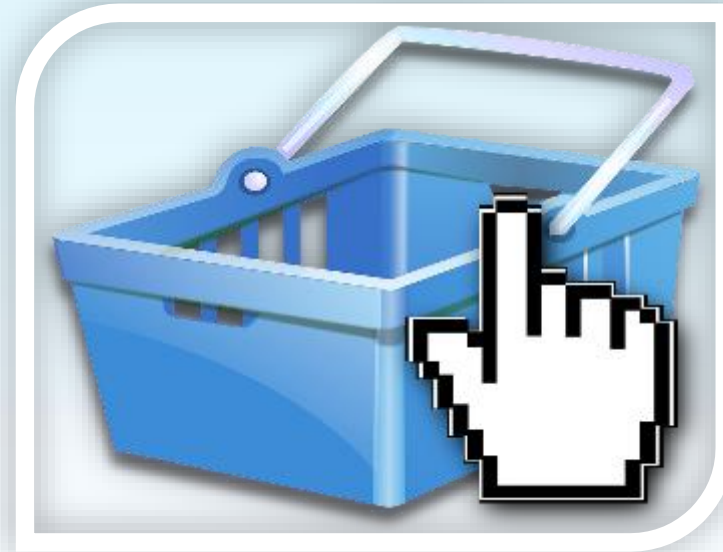
Fraud Enablers: (How are scams committed)

## 1. Phone



**31%**

## 2. Online Sales



**15%**

## 3. Email



**12%**

National Fraud Intelligence Bureau: NFIB Victim data April 2017 to March 2018

# Fraud & cyber crime in Kensington & Chelsea



**Advance Fee**



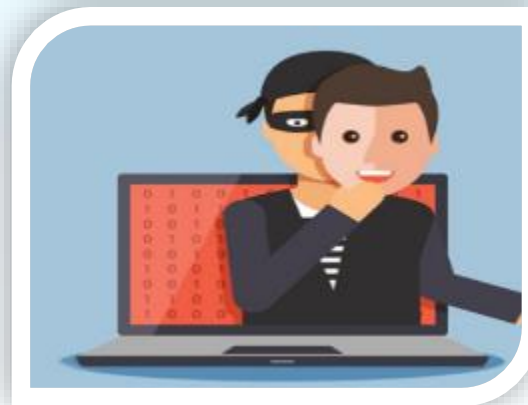
**Courier Fraud / Push Payment**



**Software Service Fraud**



**Investment Fraud**



**Payment Fraud**



**Online Shopping**

# Social Engineering

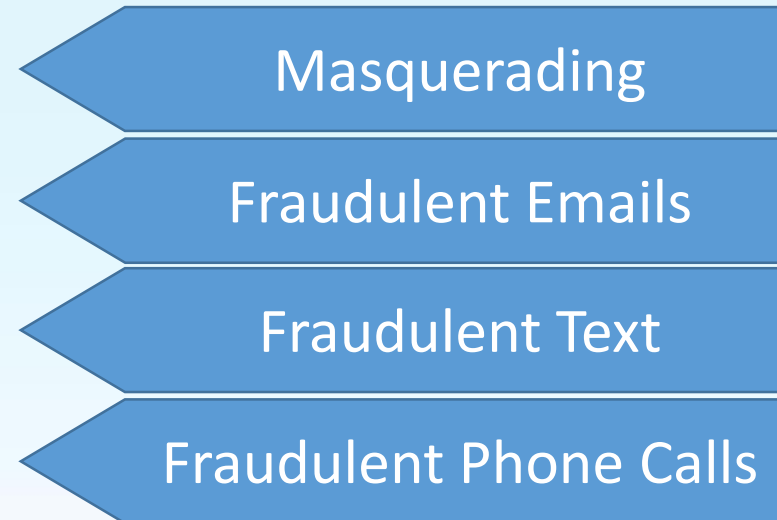
“The clever manipulation  
of the natural human  
tendency to trust.”

(hacking the human)



# Social Engineering

1. Spoofing
2. Phishing
3. Smishing
4. Vishing



# Spoofting (Disguising email or phone number)



**SpoofCard** DISGUISE YOUR CALLER ID

HOME BUY CREDITS FEATURES MOBILE APPS MEDIA HELP SIGN UP LOGIN

Calling Barack Obama as:  
**(555) 555-1212**  
Mitt Romney

## Disguise your Caller ID

Display a different number to protect yourself or pull a prank on a friend. It's easy to use and works on any phone!

**From:** cybermonday@amazon.co.uk <cybermonday@amazon.co.uk>  
**Sent:** 29 November 2018 07:59



[Your Amazon](#) [Today's Deals](#) [All Departments](#)

**Cyber Monday Sale**  
26<sup>th</sup> - 30<sup>th</sup> November New deals every day

Dear client,

As a thank you for being an Amazon customer, we have placed a £800 Amazon credit for you. We will automatically apply the balance of your credit to any purchase in the Amazon only on CYBER MONDAY SALE!

**Save up to 75%!**

**26th - 30th  
November.**

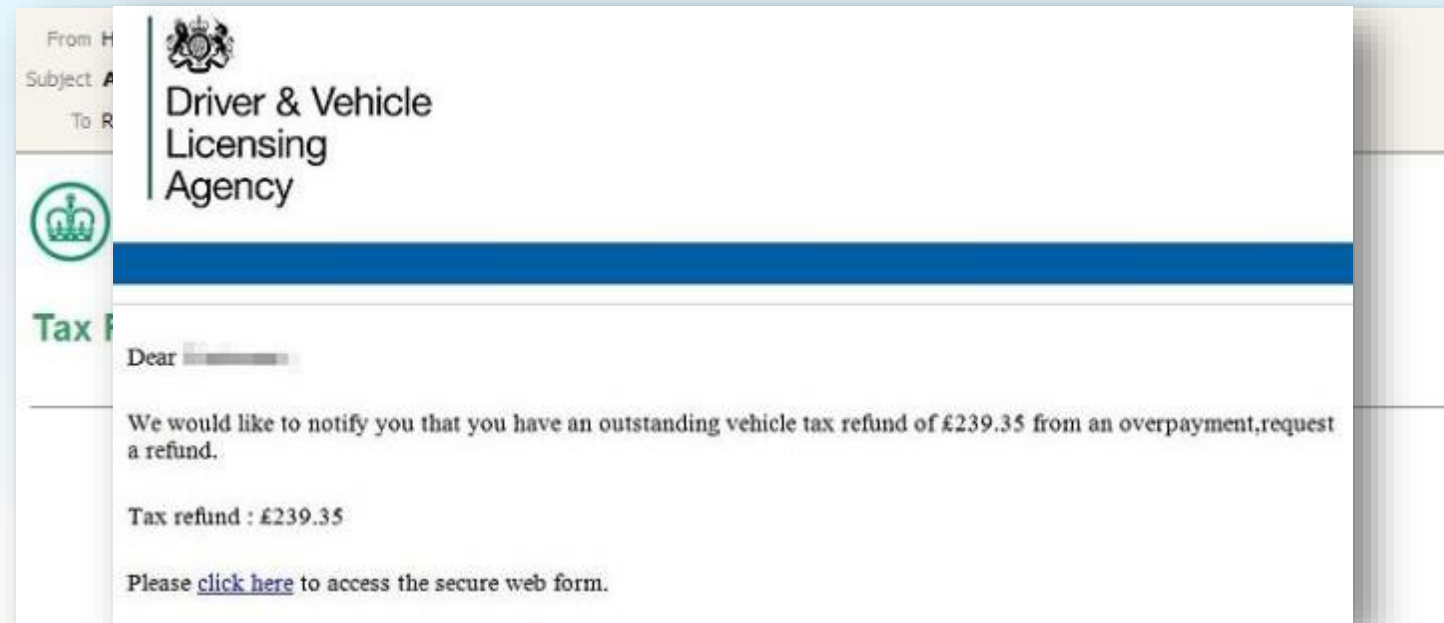
[Get your Cyber Monday coupon.](#)



© 2018 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210.

# Phishing (Scam emails)

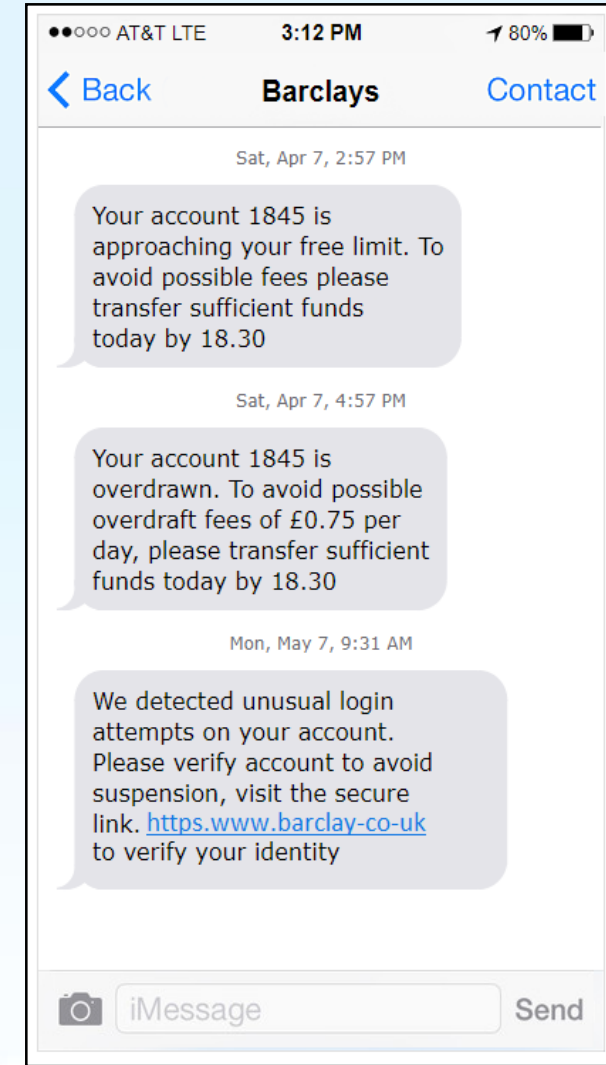
- No longer the International Prince trying to get his funds out of the country!  
More creative and accurate



# Smishing

## (Scam Text Messages)

- Phishing via SMS messages
- Free apps allow you to change your number to be anything you want.
- It will automatically appear in legitimate conversations.



# Smishing & Phishing

- Don't assume a text or email is genuine.
- Never click on links or attachments in unsolicited texts or emails.
- Don't respond to requests for personal information or bank details



# Vishing

- Scam phone calls
- They may know your basic details
- Background sound effects add authenticity
- Often put under pressure to make quick decisions



# Vishing

“Unusual activity on your account”

**“Your account  
will be shut down”**

“You will be arrested!”

“Your computer has been hacked”



# Fraud & cyber crime in Kensington & Chelsea



**Advance Fee**



**Courier Fraud / Push Payment**



**Software Service Fraud**



**Investment Fraud**



**Payment Fraud**



**Online Shopping**

# Advance Fee

Advance fee fraud is when fraudsters target victims to make advance payments for goods, services and/or financial gains that do not materialise.

## Examples Include:

Impersonation of officials  
Career opportunity scams  
Inheritance fraud  
Loan scams  
Lottery, & prize draw scams

Fraud Recovery  
Racing tipster scams  
Rental fraud  
Work from home  
Vehicle matching scams

139 Reports totalling £289,714 reported lost in RBKC in 2018.  
(Avg £2,084 per victim)



# Advance Fee

In reality, you'll never see a penny.  
Because the service/product doesn't exist.

Best case, you've only lost the advance fee.

Worst case, the scammers now have your details.

139 Reports totalling £289,714 reported lost in RBKC in 2018.  
(Avg £2,084 per victim)



# Courier Fraud

Courier Fraud January 2018 to December 2018						
Borough	Total Offences	Complete	Incomplete	Success Rate	Amount Lost	Avg loss
Kensington & Chelsea	166	41	125	25%	£745,254	£18,177
Bromley	92	44	48	48%	£405,545	£9,217
Westminster	136	35	101	26%	£371,784	£10,622
Camden	85	32	53	38%	£229,585	£7,175
Hammersmith & Fulham	67	15	52	22%	£159,444	£10,630

# Courier Fraud & Push Payment



Tax Office



Bank



Police



# Courier Fraud & Push Payment Fraud



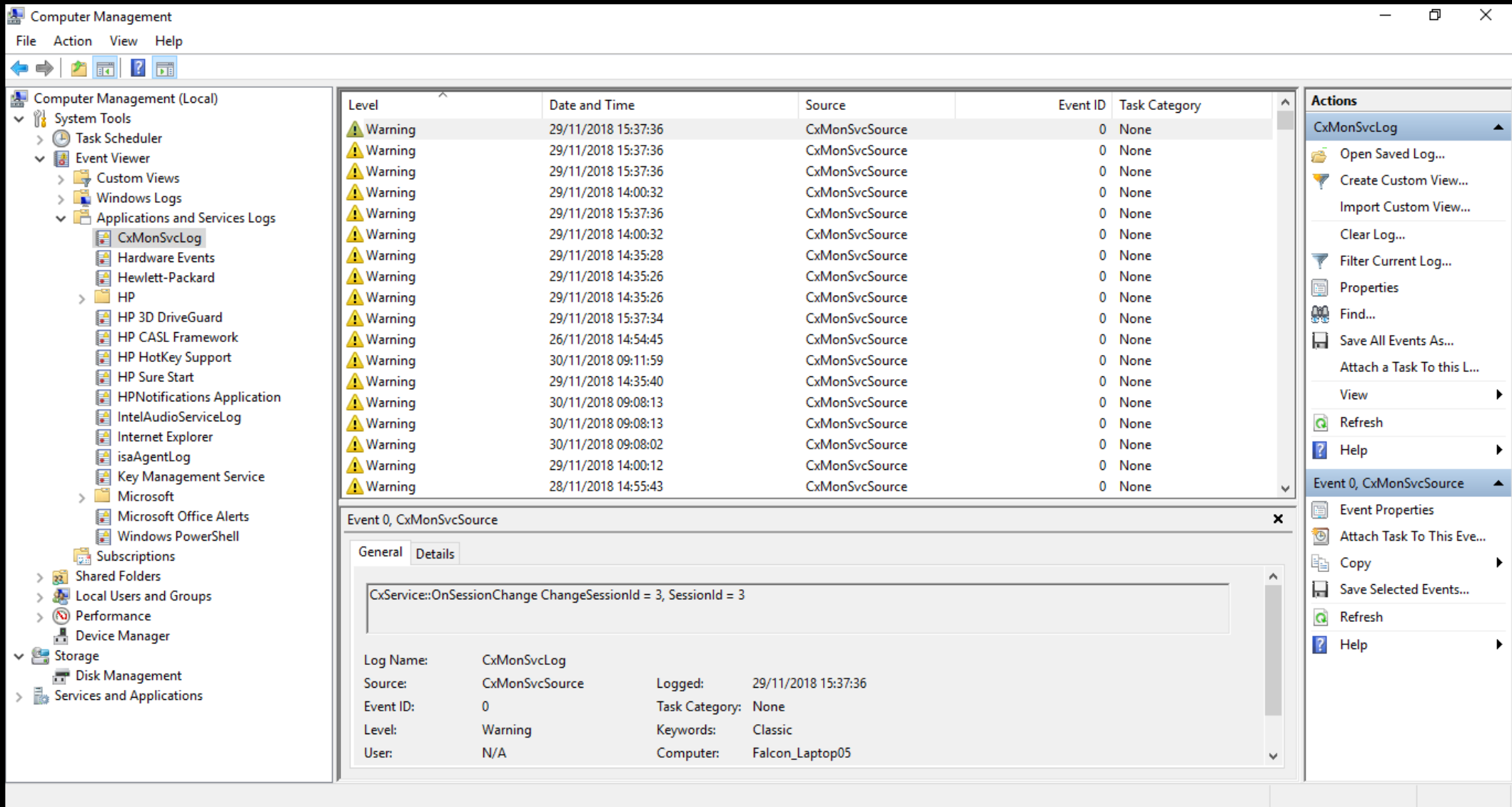
- Your bank, the police or tax office will **never** call you to ask you to verify your personal details or PIN by phone.  
Even by tapping the PIN into your phones keypad.

They would **never** ask you to withdraw or transfer money, purchase goods or offer to pick up your card by courier.  
**Hang up if you get a call like this.**

- Never hand over your PIN, money, bank cards or make purchases following an unexpected call.



# Computer Software Service Fraud



The screenshot shows the Windows Event Viewer interface. The left pane shows the navigation tree with 'Applications and Services Logs' expanded to 'CxMonSvcLog'. The main pane displays a list of 16 warning events. The right pane shows the 'Actions' menu for the selected event.

Level	Date and Time	Source	Event ID	Task Category
Warning	29/11/2018 15:37:36	CxMonSvcSource	0	None
Warning	29/11/2018 15:37:36	CxMonSvcSource	0	None
Warning	29/11/2018 15:37:36	CxMonSvcSource	0	None
Warning	29/11/2018 14:00:32	CxMonSvcSource	0	None
Warning	29/11/2018 15:37:36	CxMonSvcSource	0	None
Warning	29/11/2018 14:00:32	CxMonSvcSource	0	None
Warning	29/11/2018 14:35:28	CxMonSvcSource	0	None
Warning	29/11/2018 14:35:26	CxMonSvcSource	0	None
Warning	29/11/2018 14:35:26	CxMonSvcSource	0	None
Warning	29/11/2018 15:37:34	CxMonSvcSource	0	None
Warning	26/11/2018 14:54:45	CxMonSvcSource	0	None
Warning	30/11/2018 09:11:59	CxMonSvcSource	0	None
Warning	29/11/2018 14:35:40	CxMonSvcSource	0	None
Warning	30/11/2018 09:08:13	CxMonSvcSource	0	None
Warning	30/11/2018 09:08:13	CxMonSvcSource	0	None
Warning	30/11/2018 09:08:02	CxMonSvcSource	0	None
Warning	29/11/2018 14:00:12	CxMonSvcSource	0	None
Warning	28/11/2018 14:55:43	CxMonSvcSource	0	None

Event 0, CxMonSvcSource

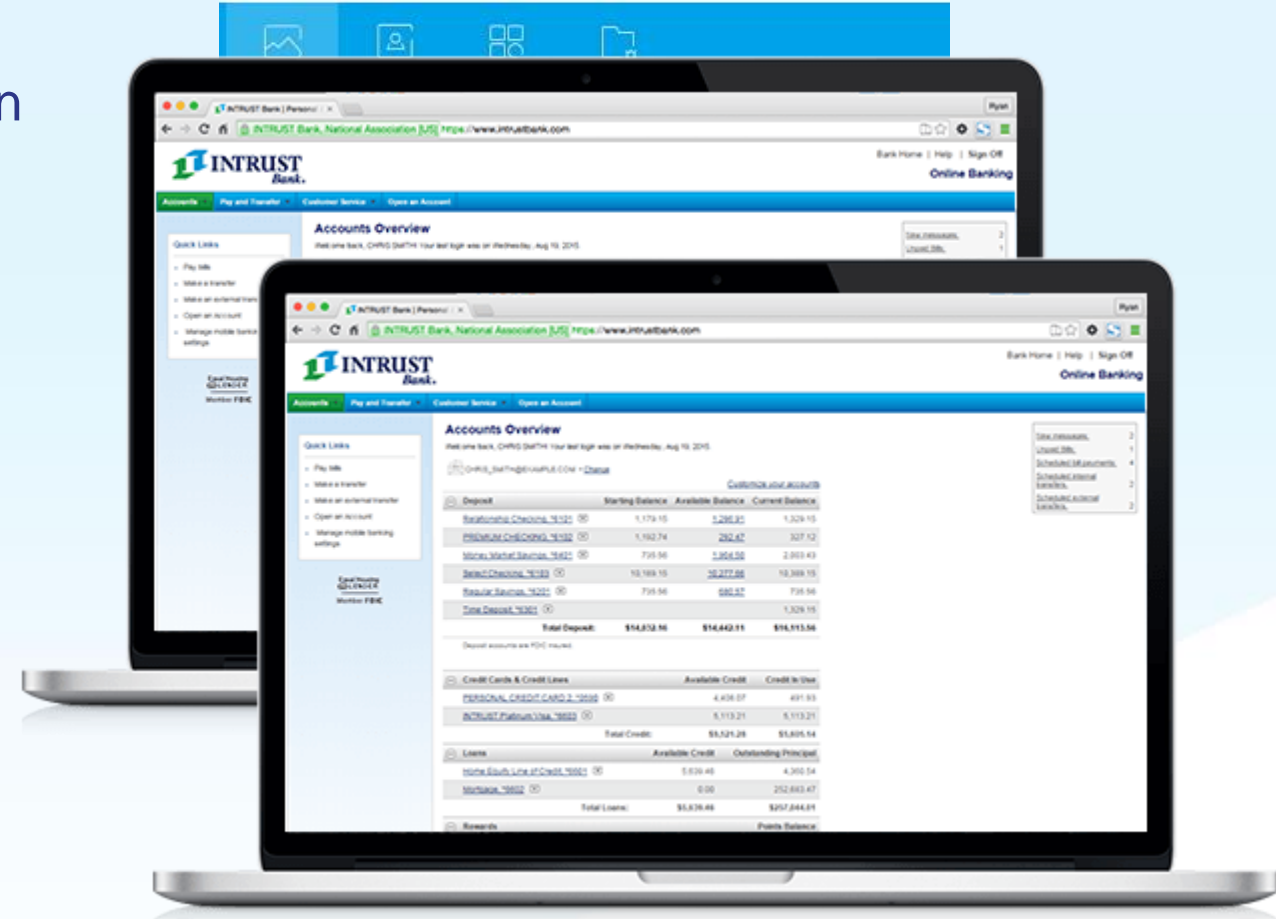
General Details

CxService::OnSessionChange ChangeSessionId = 3, SessionId = 3

Log Name: CxMonSvcLog  
Source: CxMonSvcSource      Logged: 29/11/2018 15:37:36  
Event ID: 0      Task Category: None  
Level: Warning      Keywords: Classic  
User: N/A      Computer: Falcon\_Laptop05

# Computer Software Service Fraud

- With remote access to the victims computer fraudsters now have access to everything on the victims computer including;
- Passwords
- Photos
- Emails
- Webcam
- And are able to download malware.
- They'll request payment for their “services” and encourage the victim to use online banking. – Once used, fraudsters now have access to the victims online banking.



# Computer Software Service Fraud

- Genuine computer service companies don't call people out of the blue.  
Microsoft don't have customers details on file.  
Hang up if you get a call like this.
- Don't allow people to remote access your computer.
- If you *are* having issues with your computer, contact the retailer you purchased it from
- If you're having broadband problems contact your internet service provider.



# Investment Fraud

Fraudsters call you to persuade you to **invest** in all kinds of products, including diamonds, wine or art.

They offer low risk, high rates of return and claim it's a once in a lifetime opportunity and you'll have to act quickly.

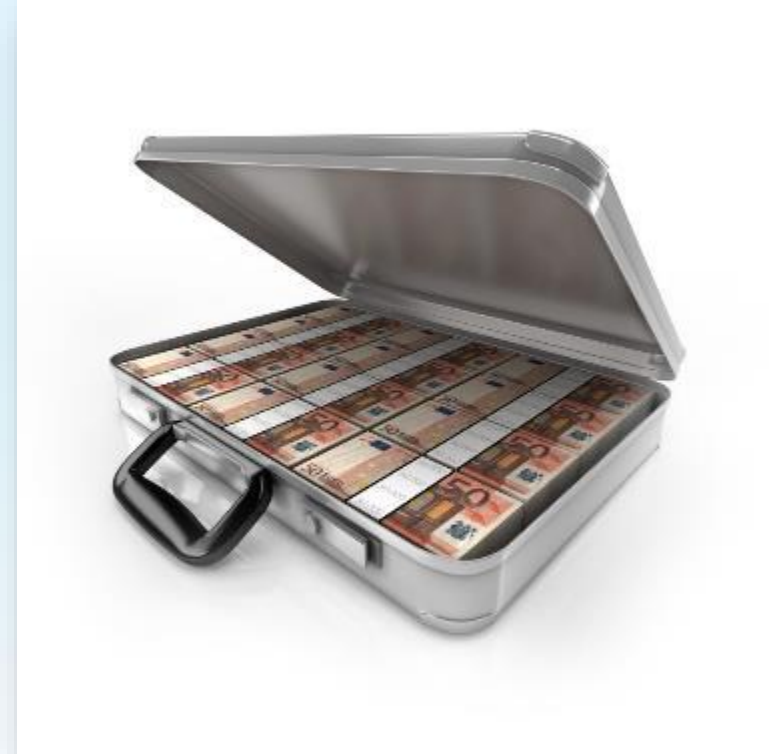
**If it sounds too good to be true, it probably is.**

Genuine investment companies will **not** cold call you.

When considering making an investment research the offer and the investment company, speak to **Financial Conduct Authority** if you have concerns

Don't be pressured into making a quick decision.

Seek **impartial** financial advice before committing to any investment.



£878,645 reported lost in RBKC in 2018.  
(Avg £30,298 per victim)

# Phone Scams – What to do...

## 1. HANG UP!



# Phone Scams – What to do...

**1. HANG UP!** 

**2. Take 5...** 



# Phone Scams – What to do...

1. HANG UP!



2. Take 5...



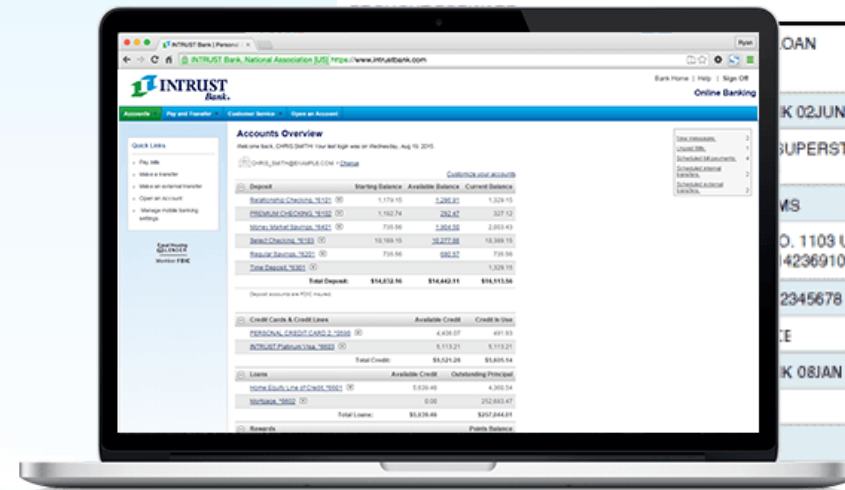
3. Verify.



Account Number: 12345678  
Sort Code: 98-00-60  
BIC: ULSBGB2B  
IBAN: GB48 ULSB 9800 6012 3456 78

Period	1 Jan 2014 to 31 Jan 2014
Previous Balance	£350.00
Paid Out	£258.05
Paid In	£1392.95
<b>New Balance</b>	<b>£1484.90</b>

Date	Type	Description	Paid In	Paid Out	Balance
					350.00



					250.00
			100.00		250.00
				30.00	220.00
				5.80	214.20
				55.00	159.20
				41.25	117.95
					121.45
			3.50		121.45
				15.00	106.45
				10.00	96.45
				50.00	45.45
			1389.45		1434.90

# Call blockers.



BT Call Protect



TalkTalk callsafe



Sky Talk Shield



Virgin



# Payment Fraud

“Mandate” or payment fraud takes place when you or an employee is deceived into changing a regular payment mandate (such as a direct debit, standing order or bank transfer), by a fraudster purporting to be an organisation you make regular payments to such as a supplier, membership or subscription organisation.

Lawyers firms and builders merchants are predominantly targeted. Emails can be spoofed or in some cases accounts are hacked and “genuine” emails are sent.

## **‘We lost £120,000 in an email scam but the banks won’t help get it back’**

In another example of a growing menace, the Scotts thought they were sending money to their solicitor’s bank account. Little did they know it went to a fraudster



▲ Never trust an email containing bank account or payment details. Photograph: Dominic Lipinski/PA

**I**t is the worst case of email intercept fraud that Money has ever featured. An Essex couple have lost £120,000 after sending the money to what they thought was their solicitor’s bank account, but which instead went to an account in Kent that was systematically emptied of £20,000 in cash every day for the next six days.

£2,131,181 reported lost to Payment Fraud in RBKC in 2018. (Avg £36,745 per victim)

Bill Bailey [Cyber crime Video](#)

# Payment Fraud

Be wary of requests for a change in bank account payment details.

Double Check email addresses.

Contact the person directly via phone to confirm change in bank details.

## **'I thought I'd bought my first home, but I lost £67,000 in a conveyancing scam'**

Howard Mollett is the victim of 'Friday afternoon fraud', an email scam that is the No 1 cybercrime in the legal sector



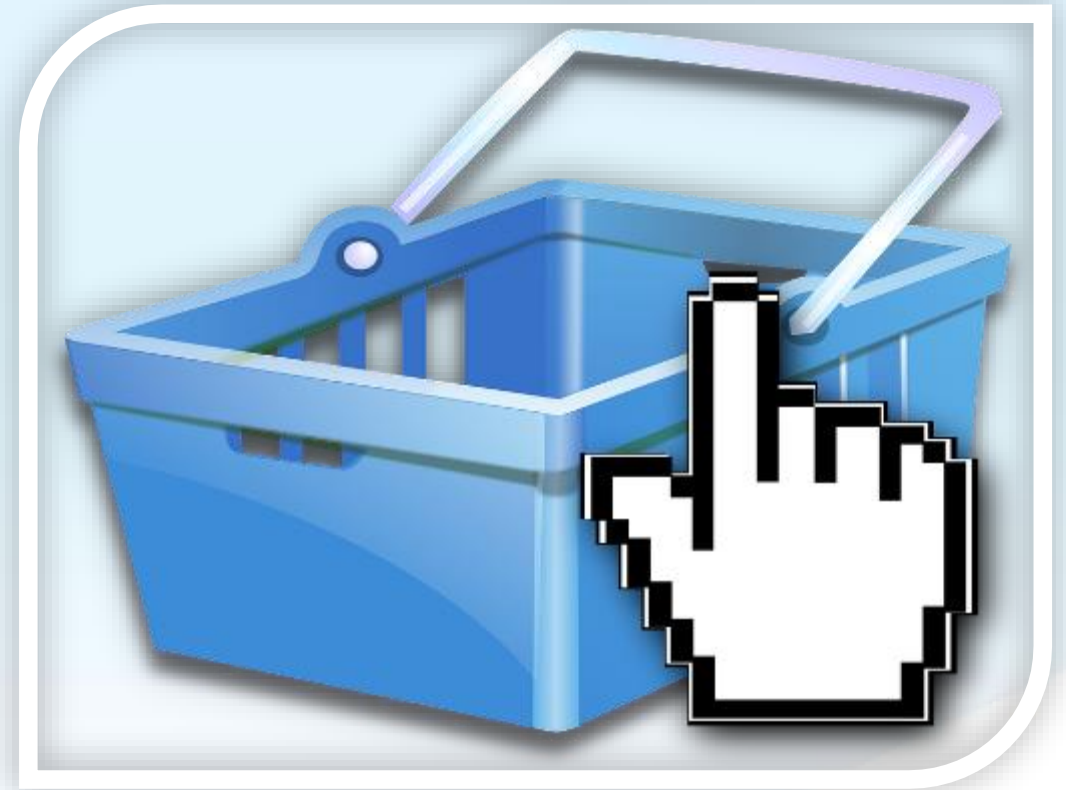
▲ Charity worker Howard Mollett was cheated out of his life savings after hackers posed as the solicitor he was using to buy his first house. Photograph: David Levene for the Guardian

A charity worker buying his first home has had his £67,000 life savings stolen after fraudsters hacked into emails sent between him and his conveyancing solicitor.

# Online Shopping Fraud

## Father duped on Ebay after he ordered £450 XBox One for his son for Christmas... but received a PICTURE of a console instead

- Peter Clatworthy, 19, from Nottinghamshire, saved for console for a year
- But his four-year-old son McKenzie will be disappointed this Christmas
- He failed to notice the misleading advert had the word 'photo' in the title
- Auction site seller even wrote 'thank you for your purchase' on the back



£242,905 reported lost to online shopping fraud in RBKC in 2018.  
(Avg £1,404 per victim)

VIDEO The little guide to safe online shopping on [YouTube](#).

# 7 Tips to reduce Cyber Crime.

1. **Have a strong password**
2. **Have an (up to date) anti virus**
3. **Update software – install patches.**
4. **Back up your data regularly.**
5. **Don't click on links / open attachments (unless verified)**
6. **Privacy settings on social media.**
7. **Don't use public Wi-Fi (for everything)**

Password	Time to Crack		
	Mac Book Pro	Conficker Botnet	Tianhe-2 Supercomputer

<https://password.kaspersky.com/>

So what constitutes a strong password?



fish    fishboat    tulip

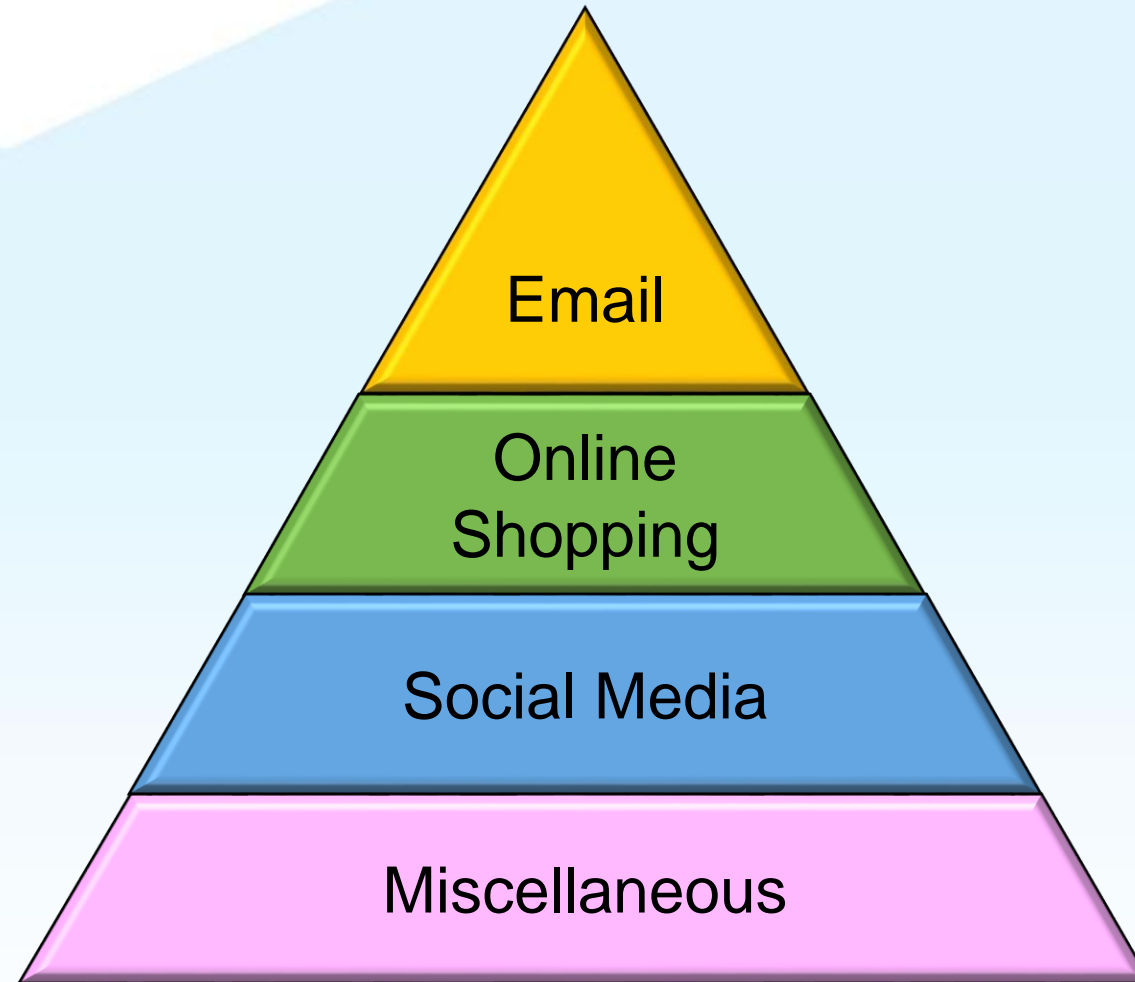
!!

1995

Password	Time to Crack		
	Mac Book Pro	Conficker Botnet	Tianhe-2 Supercomputer
oscar1990	5 mins	1 sec	1 sec
O5caRd0g!990	9 yrs	4 hrs	2 mins

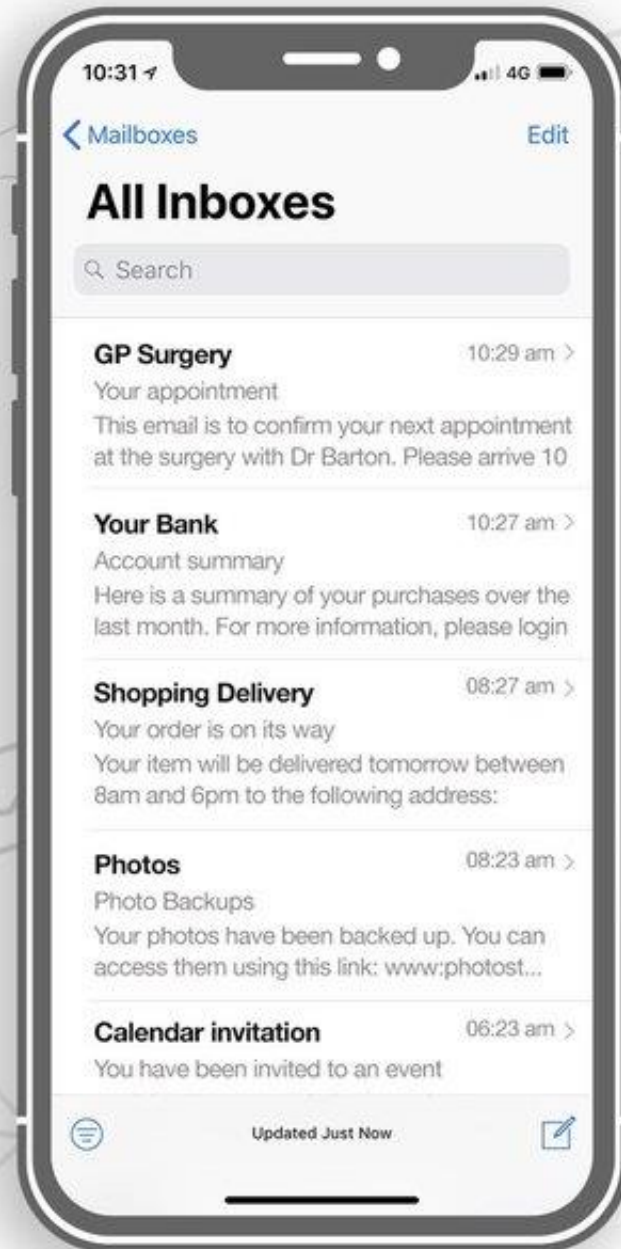
<https://password.kaspersky.com/>

# Hierarchy of Passwords



# Email accounts contain more than just your emails

Email accounts contain a wealth of sensitive information. Criminals can use your email to reset passwords or obtain personal and financial information, such as your bank details, full address or DOB, leaving you vulnerable to identity theft and fraud.



## Secure your email account with two simple steps...



**Use a strong, separate password**



**Enable two-factor authentication**

# 2 Factor Authentication

- <https://www.turnon2fa.com>
- Two-factor authentication (2FA) is an additional layer of protection beyond your password.
- It significantly decreases the risk of a hacker accessing your online accounts by combining your password with a second factor, like your mobile phone.



HOME ABOUT TUTORIALS BLOG

TeleSign  
Presents

THE ULTIMATE GUIDE TO TWO-FACTOR AUTHENTICATION (2FA)

**TURN IT ON**

Step-by-step instructions on enabling the free security feature that prevents hackers from accessing your accounts, even if they know your password.

Enter a site here **SEARCH**

Not sure what 2FA is? We've got you covered!

# FINAL POINTS.

## 1. Out of the blue? NO THANK YOU!

1. HANG UP!
2. Take 5
3. Verify.



# FINAL POINTS.

1. Out of the blue?  
**NO THANK YOU!**

2. Be Cyber aware.



# FINAL POINTS.

1. Out of the blue?  
**NO THANK YOU!**

2. Be Cyber aware.

3. Tell2

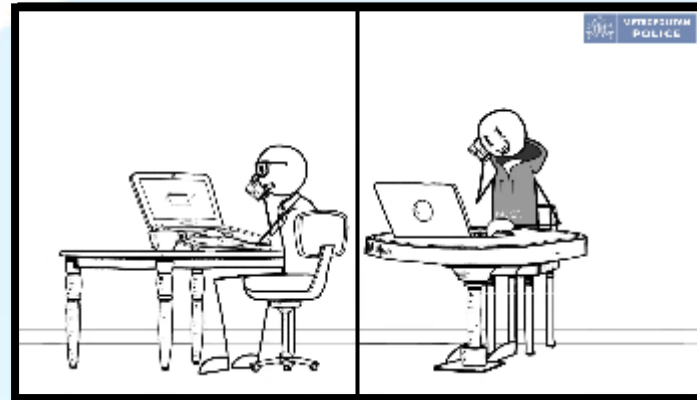




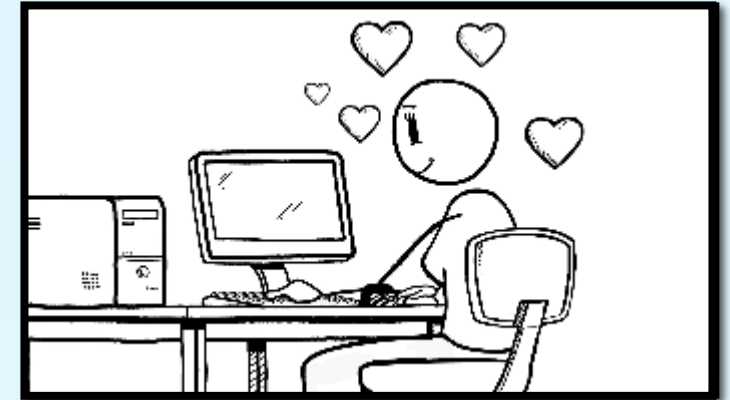




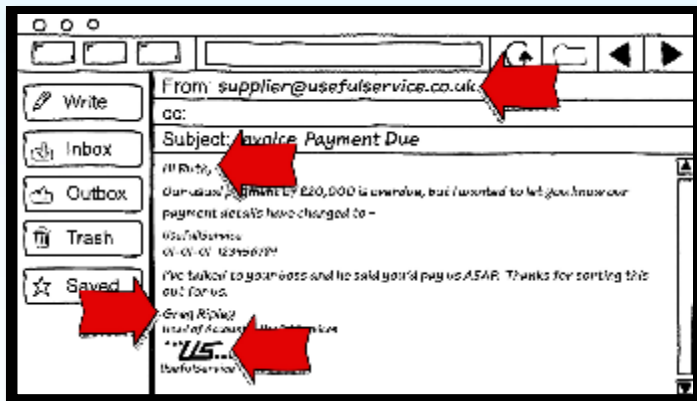
Online Shopping



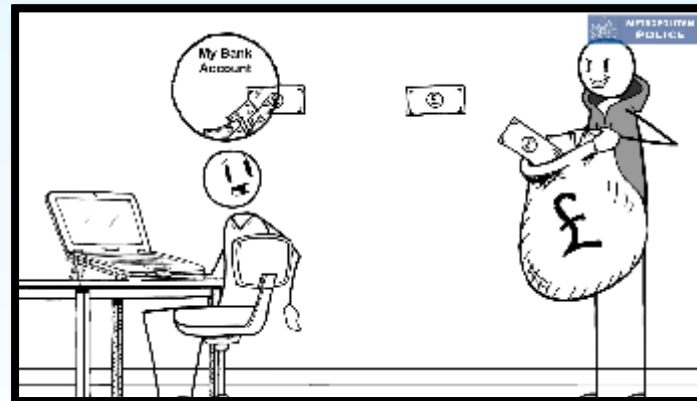
Computer Software Service Fraud



Romance/Phishing



Payment Fraud



Money Muling

[www.met.police.uk/littlemedia](http://www.met.police.uk/littlemedia)



How can we help you?



Report

Tell us about

Apply or register

Request

Feedback

Your area



Advice and information

## Fraud

Every year, the British public loses billions of pounds to fraudsters. With scams ranging from the simplest confidence trick to the most sophisticated high-tech online fraud, it pays to keep up to date with the latest news and advice. Find out more about fraud, its many types and how you can report it.



Personal fraud

Business fraud

Cybercrime

Useful contacts for advice about fraud and cybercrime

Report fraud

Online fraud

## Start reporting

Please select the option that best describes you:

I am

- A VICTIM →
- REPORTING FOR A VICTIM →
- A BUSINESS →
- A WITNESS →

**24/7 LIVE CYBER REPORTING FOR BUSINESSES**

LEARN MORE





# FALCON Prevent/Protect/Prepare Team

~

[www.met.police.uk/fraud](http://www.met.police.uk/fraud)  
[CyberProtect@met.police.uk](mailto:CyberProtect@met.police.uk)