Information Network Bulletin

Edition 4

2016/17

Welcome to the latest edition of the Information Network Bulletin brought to you by Croydon Council's Trading Standards team.
In addition to general news from the team, it includes details of some of the latest scams and fraud alerts which we have become aware of in recent months.

We hope that you find it useful.

Courier Scam

The courier scam is when fraudsters call and trick you into handing your cards and PIN numbers to a courier on your doorstep. There are many variations of the scam, but it usually follows this method:

A fraudster will cold call you on a landline, claiming to be from your bank or the police. They state their systems have spotted a fraudulent payment on your card or it is due to expire and needs to be replaced.

In order to reassure you that they are genuine, they suggest that you hang up and ring the bank/police back straight away. However, they don't disconnect the call from the landline so that when you dial the real phone number, you are actually still speaking to the fraudster.

They then ask you to read out your PIN or type it on your phone keypad. They may ask for details of other accounts you hold with the bank or financial service provider.

Finally, they send a courier to you to collect your bank card. The fraudster will have then obtained your name, address, full bank details, card and PIN.

Protect yourself against courier fraud

- Your bank will never send a courier to your home
- Your bank and the police will never collect your bank card
- Your bank and the police will never ask for your PIN
- If you receive one of these calls end it immediately

National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

ALERT

Fraudsters are sending out a high number of phishing emails to personal and business email addresses purporting to be from 'Migrant Helpline'.

The email address sending the majority of emails is noreply@yeshivadonations.com, however multiple email addresses have been seen. Although Migrant Helpline is a genuine charity, fraudsters are using it to trick members of the public into becoming victims of this fraud.

It should be noted that this fraud is in no way related to the real charity.

The subject line currently is 'Thank you for choosing to donate to Migrant helpline'

The message body reads as the following:

Thanks again for donating

We're sending it straight to Migrant Helpline so you'll be making a difference very soon.
Your donation details:
First name: ****
Last name: ****
Tel. *********
Amount: £196
Donation Reference: 09493495

If you have any questions about your donation, please follow this link and download Your (Donation Reference 09493495), with the transaction details listed above.
With your help, YeshivaDonations can continue to work in Syria and neighbouring countries to deliver clean water and life-saving supplies to millions of people.

Your generosity is bringing much-needed assistance to families who have lost everything as a result of the crisis in Syria.

Warm regards,
YeshivaDonation

The first name, last name and telephone number are targeted and appear to be correct for those they are sent to.
Once the link is clicked, a well known Trojan (Ramnit) is downloaded onto the victim's device. This malware is equipped to target and steal personal and corporate banking details.

PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent your device(s) from becoming infected.

Please consider the following actions:

Don't click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication.

Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.

Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to is not left connected to your computer as any malware infection could spread to that as well.

If you think your bank details have been compromised, you should contact your bank immediately.

*If you have been affected by this, or any other fraud, report it to Action Fraud by calling **0300 123 2040**, or visiting www.actionfraud.police.uk.*

FEEDBACK

*The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: **www.surveymonkey.com/r/FeedbackSDU**. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send to*

***NFIBfeedback@cityoflondon.pnn.police.uk**.*

CAN YOU HELP?

Trading standards are interested in receiving leaflets advertising home improvement works that you may receive through your door. We'd really appreciate it if you could either send the leaflet in to us or e-mail a scanned version together with the date that you received it (or a rough date) and where you live.

Send them through to us at:

Croydon Trading Standards
Leaflets
Bernard Weatherill House
8 Mint Walk
Croydon CR0 1EA

Or email a scanned copy to trading.standards@croydon.gov.uk

Scam Alert

NATIONAL TRADING STANDARDS
Scams Team

5 Common Scams: How to Stay Safe

New reports have shown that the nation lost a total of £755 million to financial fraudsters last year alone.

According to the Financial Ombudsman Service (FOS), three-quarters of criminals target their victims via cold calls or online.

Phone calls make up around 57% of cases, while the rest are either through online contact or email.

Here are the five most dangerous scams to look out for, according to FOS.

1, Upfront payment fees

When criminals ask you to pay fees to release compensation payouts or loans with traders disappearing after payments are made.

2. Fake services or invoices

Where people pay charges to remove fake computer viruses and receive fake advertising invoices.

3. Goods not being received

From purchases made through social media or auction websites.

4. Vishing

Fraudulent phone calls where the criminals attempt to get personal details such as credit card numbers to renew a subscription or for information about personal debt.

5. Subscription traps

Victims are tricked into signing up to subscription services for a free or discounted trial. The criminals will take a whole load of large payments, often changing their company name to mislead you.

How can I tell it's a scam?

Criminals generally use the same set of tactics, making you think that something's gone wrong and that the fraudster has the power to put it right. What's more, they can trace your personal information through social media or spyware.

However, there are a few classic signs that you're being targeted by a scam. Keep an eye out for dodgy spelling and grammar, pressure for you to act quickly and promises of payouts or impossibly high returns on investments.

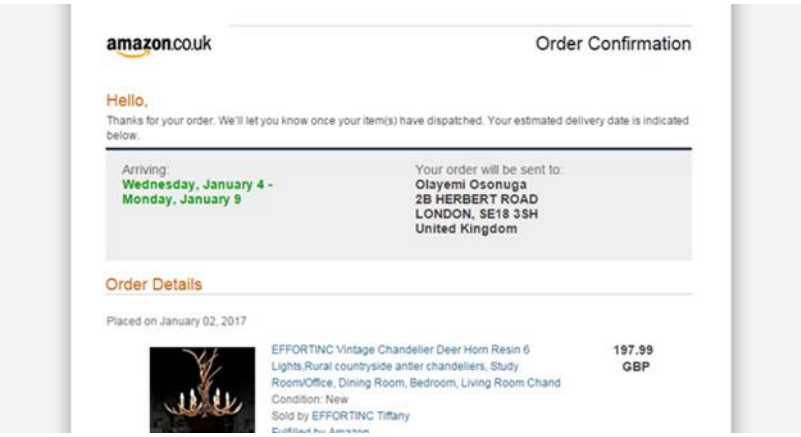
Fake Amazon emails claim you have placed an order

Several reports have been received by Action Fraud from victims who have been sent convincing looking emails claiming to be from Amazon.

The spoofed emails from "service@amazon.co.uk" claim recipients have made an order online and mimic an automatic customer email notification.

In one example below, the scam email claims recipients have ordered an expensive vintage chandelier. Other reported examples include; Bose stereos, iPhone's and luxury watches.

The emails cleverly state that if recipients haven't authorised the transaction they can click on the help centre link to receive a full refund.
The link leads to an authentic-looking website, which asks victims to confirm their name, address, and bank card information.


amazon.co.uk Order Confirmation

Hello,

Thanks for your order. We'll let you know once your item(s) have dispatched. Your estimated delivery date is indicated below.

Arriving:
Wednesday, January 4 - Monday, January 9

Your order will be sent to:
Olayemi Osonuga
2B HERBERT ROAD
LONDON, SE18 3SH
United Kingdom

Order Details

Placed on January 02, 2017

EFFORTINC Vintage Chandelier Deer Horn Resin 6 Lights,Rural countryside antler chandeliers, Study Room/Office, Dining Room, Bedroom, Living Room Chand
Condition: New
Sold by EFFORTINC Tiffany

197.99 GBP

One victim lost £750

One victim reported entering his Nationwide banking details and later found out £750 had been stolen from his account.
After the victim notified Nationwide they cancelled the card and refunded the money in full.

Amazon says that suspicious e-mails will often contain:

Links to websites that look like Amazon.co.uk, but aren't Amazon.co.uk.
Attachments or prompts to install software on your computer.
Typos or grammatical errors.
Forged (or spoofed) e-mail addresses to make it look like the e-mail is coming from Amazon.co.uk.

In addition

Amazon will never ask for personal information to be supplied by e-mail.
Read more about **identifying suspicious emails** claiming to be from Amazon.

BEWARE OF COLD CALLS FOR BOILER COVER

At this time of year keeping our houses warm and ensuring there is a plentiful supply of hot water is important to all of us. However, it appears that some businesses look to take advantage of this to lure people into taking out boiler protection cover with them.

Reports have been made around the country, about various businesses, who allegedly cold call people at home, by telephone, and try to frighten or pressure them into taking out boiler cover with them.

People are told things such as:

- Your boiler is out of warranty and you have no cover if it breaks down
- Your boiler cover has expired and you need to renew it now
- The card you used to pay for your boiler cover last time has expired and we need your new card details
- Your boiler is due a service and we need to take payment now

Often, these calls are received by elderly and/or vulnerable person who, frightened by what they have been told, will give their card details to the caller concerned that they may find themselves without heating and/or hot water.

When the paperwork then arrives confirming their new boiler cover and the payment that they have made, many will then realise that the call was not from their existing provider and that they now have a second, un-wanted policy which they must act quickly to cancel in order to obtain a refund of their money. Sometimes these refunds can take a long time to materialise, which is not good if you have a limited income and find your-self a few hundred pounds out of pocket whilst you wait for the money to be returned.

So don't be panicked into taking out cover over the phone!

Be prepared:

- Make your own arrangements for boiler cover by contacting someone you know, or whose details you have found for yourself, so you know who you are dealing with. If you have a local plumber who looks after your boiler, talk to them about being called out in emergencies.
- If you have a policy that is renewed annually, the provider will write to you to let you know when it is due for renewal and how much you will need to pay.
- If you get a telephone call advising that your cover or warranty has expired. Ask for their business name and phone number and tell them you will ring them back. Then go and check your paperwork to see if your cover really has run out. If it hasn't and they call again, ask them to take you off their calling list as you want no further telephone calls from them.

If you are registered with the Telephone Preference Service (TPS), you can report the unwanted cold call to them; and if the caller has said someone that isn't true, do report this to them.

If you are trying to source someone to carry out a boiler service, try contacting:

Age UK
Tel: 020 8683 7120, Monday – Friday 9.30am to 4.00pm.

Buy With Confidence
www.buywithconfidence.gov.uk
E-mail : admin@buywithconfidence.gov.uk
Tel : 03454 040506

Being asked for payment by i-tunes vouchers? Tell them to go whistle!

We have received several reports from members of the public who have received telephone calls from person claiming to work for HMRC (the tax office), or other organisations claiming that the person owes them money and demanding immediate payment. They terrify the person they have called by saying they will be arrested by the Police if they do not pay up immediately.

Strangely, however, they do not want card payments, they tell the person to purchase i-tunes vouchers and give them the voucher codes over the telephone.

Beware, these callers are fakes and as soon as you give them the voucher code the money is gone and not retrievable. So if you get a call like this – hang up!

Remember:

Information about ourselves and our lifestyles is very valuable. We give this information out every time we fill out a form, survey, questionnaire, or enter a competition

Our personal information is bought by both honest businesses and fraudsters who want to target us. Once it's out there we can't take it back. We will get more unwanted post, emails and telephone calls from legitimate businesses and also fraudsters trying to trick us. It is increasingly difficult to tell the difference.

Our advice:

- **Provide the minimum information to companies you do business with. Don't be afraid to decline personal details, such as your date of birth, if you don't believe the business has a legitimate reason for requesting it.**
- **Avoid filling in marketing surveys or questionnaires in the street, on the doorstep, over the telephone or online.**
- **When you fill out your annual electoral registration form, opt out of the open (or edited) register. The open register is sold to businesses for marketing purposes.**
- **When you buy goods and services online, opt out from receiving marketing emails and don't allow your details to be shared with 'carefully selected' third parties. You may need to tick or un-tick a box at the bottom of the web page.**

Find out more about Community Safety

Would you like more up-to-date information on crime and safety in the borough?

Visit www.croydon.gov.uk/subscribe - and sign up for our online newsletter - Crime and safety news.

Nearly three quarters of consumers risk missing dangerous product recalls

Despite a number of high profile safety notices and product recalls issued during the last year, nearly three quarters of British consumers say that they don't always register their electrical appliances.

In 2016 alone, there were 61 recall notices issued for electrical products in the UK, which means there were millions of potentially dangerous products in UK homes.

Registering an electrical product allows manufacturers to contact consumers directly in case of a safety concern, such as a product recall. Without registering, millions of British consumers could be unwittingly putting their lives at risk if they continue to use a dangerous recalled product.

The reasons why three quarters of people are not always registering vary from "It's too much hassle," to "I meant to but I forgot" and "I don't think it would have any benefits". Many consumers seem to be put off by the thought of registration, with more than one in three preferring to do household chores such as ironing or taking out the bins rather than register their large appliance online.

Only one third of consumers said they feel it is risky not to register a tumble dryer, but in the last year alone over five million potentially dangerous tumble dryers have been recalled in the UK alone.

Given the numbers of people not registering their appliances, it's no surprise that the success rate of recalls is low. Previous research undertaken by Electrical Safety First show that the success rate is rarely more than 10% to 20%, despite the huge risks of electrical shock, fire or even death that faulty electrical items can present.

Low registration levels may not be the only reason for a low response rate for recalls. One third of consumers said that they would continue to use a washing machine, even after it had been recalled. Of those who would continue using a recalled machine, one third said that they would use it if it continued to work properly and one third said that it would be too much hassle to go without. One in seven would continue to use it if they hadn't heard of a serious incident of fire or shock.

To check if an electrical item has been recalled visit electrical safety first and to register an appliance, visit register my appliance (www.registermyappliance.org.uk)

****

Was this bulletin helpful?

Contact Trading Standards to request a free door sticker advising cold callers that they are not welcome. If you are a victim of scam mail, contact us to receive a free copy of our toolkit on how to avoid falling victim and how to stop the letters.

Additionally, please let us know what you think of this bulletin and what Trading Standards topics you would like to see covered in future editions.

Contact Trading Standards: Tel: **020 8407 1311**
Email: **trading.standards@croydon.gov.uk**

Citizens Advice Consumer Service: Tel: **03454 04 05 06**
Web: **www.citizensadvice.org.uk**