POLICE SCOTLAND
Keeping people safe

Business Watch

Police Scotland Business Advice

February 2022

Welcome to our second issue of 2022. Where has the time gone!

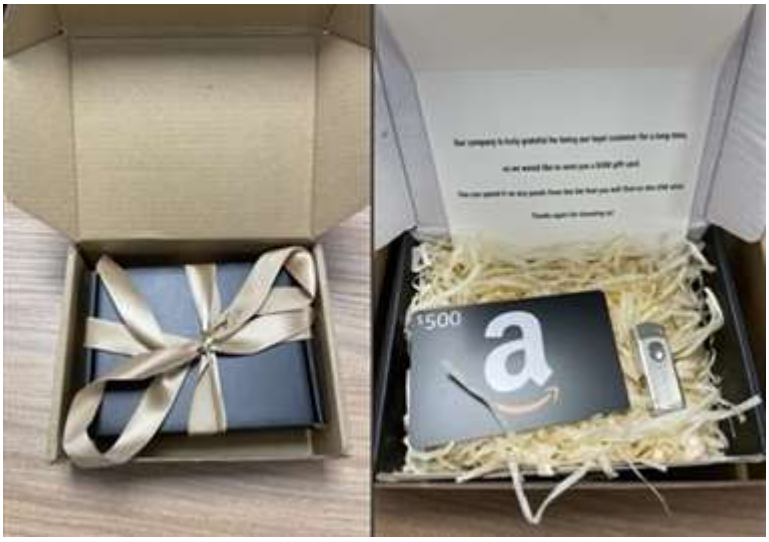
We continue to see a variety of scams and frauds appearing, many new and many a variation on older versions. We will continue to send advice and information for you to read and share. We appreciate all the positive comments received as well as information on scams we had not seen before.

Given how popular our newsletter has become, we feel we may have outgrown the title ‘Business Watch’ so be ready for a few changes next month!

Malicious USB Drives

We have been made aware of an active Russian cyber espionage campaign targeting our industry (Critical Infrastructure).

Packages are being delivered that contain a fraudulent thank you letter, a counterfeit Amazon gift card, and a USB device (shown below).



The letter instructs the recipient to use the Amazon gift card on any of the goods listed on the enclosed USB.

The enclosed USB is commercially available and known as a “BadUSB” or “Bad Beetle USB”. There is a “LilyGO” logo typically found on the device that would help identify it.

When plugged into a computer system, the USB device automatically injects a series of keystrokes to download and execute malware to compromise the user’s system and company network.

Thank you to James at RigNet for sharing this.

As part of Cyber Scotland Week 2022 Neighbourhood Watch Scotland brings you a number of webinars delivered by Police Scotland.

Below you will find a brief description on each event, as well as a link to register your place to attend.

Online Safety Guidance
Learn how the internet is continually evolving and how criminals can use this to their advantage.

Topics covered will include:
✓ Passwords
✓ Privacy Settings on Apps
✓ Using Public Wi-Fi
✓ Tips and advice to help you stay safe online

Register here - https://www.eventbrite.co.uk/e/online-safety-guidance-tickets-251174518747

Their Safety, Our Responsibility
As a parent you play a key role in helping your child stay safe online. Find out how you can support your child and speak to young people about online safety in a positive way.

Register here - https://www.eventbrite.co.uk/e/their-safety-our-responsibility-tickets-251417214657

Scams and Digital Footprint
Criminals are experts at impersonating people and organisations.

Safeguard yourself in the digital world and enhance your understanding about online safety, scams and your digital footprint.

Topics covered will include:
✓ Scams
✓ Phishing
✓ Sextortion
✓ Online Grooming
✓ Digital Footprint
✓ Reporting mechanisms

Register here - https://www.eventbrite.co.uk/e/scams-digital-footprint-awareness-tickets-252131460987

Don't let scammers tug your heartstrings to get at your purse strings!

With pandemic restrictions lowered or removed entirely, many expect this Valentine's Day to see a surge of star-crossed lovers seeking to make a connection compared to last February, when the country was under lockdown.

According to figure, Romance Scam incident reports increased by 40% last year, with £73.9m lost during that period, and experts expect this trend to continue in 2022. Many believe the figure is much higher, with many people, too embarrassed to admit they have been scammed.

Every year, scammers try to tug at our heartstrings to get at our purse strings, and the loneliness and isolation brought about by lockdowns means more people are looking to make romantic connections.

These scams regularly involve some form of 'catfishing' - the act of luring someone into a relationship by constructing a fictional online persona. This is where the intended victim is befriended on the internet and eventually convinced to assist their new love financially by sending them money.

Dating sites and social media platforms such as Facebook and Instagram are two of many hunting grounds used by romance fraudsters. A common tactic is to pretend to have a job that requires long periods of travel, for example a nurse working overseas, someone in the armed forces, or an offshore oil-rig worker. Romance fraudsters are patient – they might groom victims for months before they attempt to steal their money, having built a relationship and established trust. Unlike with most frauds, the victim might initially feel like they're in control and in a position of relative power, as romance fraudsters will typically pitch themselves as vulnerable or in need of help. They often ask for help for an issue with a visa, health problems or flight tickets. Victims are typically convinced to make multiple payments to assist.

How to protect yourself:

Stay on site, keep all communication on the dating website you are using.

Don't be convinced by profile pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/.
Do your own research on the person, are they members of any other social networking sites? Can you confirm what they are telling you about themselves, where they work or where they live?

Never send money to someone you have not met in person and be extremely wary of giving money to someone you have recently met, particularly if you have only recently started a relationship with them.

Be wary of anyone asking you to receive money on their behalf and transferring it on. They may be using you to launder money.

Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret

Mobile Phone Courier Fraud

We have seen a re-occurrence of mobile phone courier fraud following incidents in Aberdeen and Portlethen.

The resident received a parcel from a well-known courier company but was unaware of having ordered anything. A few moments later she had a knock on the door from a fraudster dressed in hi-vis and with false identification asking for the phone back claiming it had been delivered by mistake.

This is a scam – do not hand over the parcel.

The resident contacted her mobile phone provider who confirmed three brand new i-phones had been ordered from her account.

Delivery scams are one of the sophisticated methods fraudsters are using to leave victims out of pocket. The scam involves criminals ordering and then attempting to intercept - or trick you into handing over - high-value packages. It normally happens when criminals manage to obtain your personal details to place the order. It can be one consequence of identity theft.
If a courier unexpectedly comes to collect an item at your home, do not hand it over.

Check their credentials and call the company they claim to be representing. If you have any fears, contact the police.

QNAP NAS DeadBolt Ransomware Alert

QNAP Network Attached Storage (NAS) devices are a particular product that a number of ransomware operators are currently targeting. Previous strains have included QLocker and ech0raix, the latter was infecting systems just as recently as December 2021. The current strain that has been actively infecting systems recently is named DeadBolt. It is particularly severe given that it was reported that infections were caused through exploitation of a zero day.

For more details –

https://www.sbrcentre.co.uk/qnap-nas-deadbolt-ransomware-alert

Royal Mail Fraud

Criminals are pretending to be the Royal Mail and telling innocent individuals that there is a parcel waiting for them which they must pick up. However, the text asks those who receive it to pay a settlement fee to avoid their package being sent back. We are reminding everyone to look out for such scams as anyone with a mobile phone could be a target.

In the text, the scammer says: "Royal Mail: Your parcel is awaiting delivery. Please pay the £-- settlement fee to avoid your parcel being returned to sender."

The scam text also includes a link which sends those who receive it to a fake Royal Mail page that asks for their personal information and banking details.

Although the text and website may look real, it is a convincing scam which is tricking individuals into giving away their personal information.

The first step of the scam is to invite you to enter your postcode before asking for your full name, delivery address, email address, date of birth and mobile number. This information is fed directly to scammers who could use it commit identity fraud.

Cleverly, the scammers even tell you that your redelivery request has been 'processed successfully,' confirming the new date and asking you to press 'exit' – this redirects you to the official Post Office website, making this fake even more plausible.

The scammers can now attempt to steal money directly from your account.

If you receive a suspicious message via email, website or text message, you can take the following actions:

Email
If you feel unsure about an email you have received, you can forward it to the Suspicious Email Reporting Services at report@phishing.gov.uk

Website
If you have come across a website which you think is fake, you can report it here - https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

Text message
Report suspicious text messages for free to 7726. Your provider can investigate the text and take action if found to be fraudulent.

WhatsApp Fake Message Scam

The scam usually involves a WhatsApp message, but can also be a call or text, from someone claiming to be a family member or friend. Their main aim is to encourage recipients to transfer money.

In most cases, a person purporting to be a family member, often a daughter or son, asks for money. Typically, the reason given is they are short of money or late paying bills, so ask the recipient to transfer money into an account.

This is backed by a story that he or she has recently changed their phone or phone number to explain the use of a different number being used. They may even claim their banking apps have been frozen.

The scam is taking advantage of a person's willingness to help. Just this week in Aberdeen, £2,500 was lost by one victim alone.

Police are asking people to alert family members to the scam, particularly those who are elderly. If you get one of the scam messages, members of the public are advised to contact family members on their usual phone numbers to check.

If you receive a suspicious message via email, website or text message, you can take the following actions:

Email

If you feel unsure about an email you have received, you can forward it to the Suspicious Email Reporting Services at report@phishing.gov.uk

Website

If you have come across a website which you think is fake, you can report it here - https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

Text message

Report suspicious text messages for free to 7726. Your provider can investigate the text and take action if found to be fraudulent.

Third Sector – Cyber Resilience

We have created a selection of free webinars for third sector organisations to educate themselves in the field of cyber security. Firstly, there is the 'Introduction to Cyber Learning' webinar. This will go back to the basics on general cyber security tips, what to look out for, and what mitigations organisations should begin to put in place to stay cyber safe. Secondly, there is 'Introduction to Incident Response' webinar. Here we will discuss what incident response is, why it's a necessary implementation to every business, and how businesses can begin implementation.

https://www.sbrcentre.co.uk/scottish-third-sector-cyber-resilience

In support of many of the campaigns attached to this edition of Business Watch are a number creative assets that your company can use to promote fraud awareness among staff and clients. Consider using the Take 5 campaign graphics on email signatures and on your intranet. The full Take 5 Business Toolkit can be found at

www.takefive-stopfraud.org.uk

Get help and report a scam

If you think you have uncovered a scam, have been targeted by a scam or fallen for a scam, there are many authorities you can contact for advice or to make a report.

In the first instance, you should contact your bank immediately on a number you know to be correct, such as the one listed on your statement, their website or on the back of your debit or credit card.

Report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6400.

Every report assists police investigations, provides intelligence, informs national alerts that protect all communities, disrupts criminals and reduces harm.

In the UK you can forward scam text message to OFCOM on 7726 (free of charge), and forward suspicious emails to report@phishing.gov.uk

And don't forget to share your experience with friends and family to make sure they don't fall for the same scam.

Financial Conduct Authority (FCA)

In the UK, a firm must be authorised and regulated by the Financial Conduct Authority (FCA) to do most financial services activities.

Financial Conduct Authority (FCA) www.fca.org.uk or 0800 111 6768
www.fca.org.uk/scamsmart

Financial Service Compensation Scheme (FSCS)
www.fscs.org.uk

Financial Ombudsman Service
www.financial-ombudsman.org.uk

National Trading Standards
www.nationaltradingstandards.uk/work-areas/scams-team/

Scottish Business Resilience Centre App Launched

Reminder that recently the SBRC launched a new app to provide advice and support for businesses to do everything they can to stay safe – online and offline. Through targeted push notifications, businesses that download the app will be informed of credible threats to their operations including cyber threats, traffic, and protestor activity, and be given accurate sector-specific guidance within minutes.

https://www.sbrcentre.co.uk/scottish-business-resilience-centre-app-launched

---

TRADING STANDARDS SCOTLAND BULLETIN

Business advice and Scam Bulletins from Trading Standards Scotland can be found at

https://www.tsscot.co.uk

Aberdeenshire Trading Standard Bulletins can be found on the following link

http://publications.aberdeenshire.gov.uk/dataset/trading-standards-crime-and-scams-bulletin

Sign Up for Neighbourhood Alert for free

A great way in which Police can share information is via the Neighbourhood Alert system, which is delivered by Neighbourhood Watch Scotland. This enables us to send out e-mail messages relating to local crime trends and share crime prevention advice quickly and effectively to a wide audience. The information can also be targeted to particular groups, streets, or communities as required.

Anyone can sign-up to receive these e-mail messages, either individually or as a community group. The sign-up process allows you to specify the type of information you are interested in and from what source. This is coordinated by our partners in Neighbourhood Watch Scotland, who work with a range of partners in the public sector to provide information not only on crime, but also about community safety and resilience. We only send out messages which contribute to keeping you informed and safe.

Simply visit
www.neighbourhoodwatchscotland.co.uk

Crimestoppers - https://crimestoppers-uk.org/

Tel. 0800 555 111

SPEAK UP. STAY SAFE - CRIMESTOPPERS are an independent charity that gives people the power to speak up to stop crime 100% anonymously.

ARE YOU READY FOR A LIFE CHANGING CAREER? -
http://www.scotland.police.uk/recruitment/police-officers/

As always please share the above information with your colleagues.

Should this bulletin be sent to one of your colleagues as well as you? If you are 'moving on' please let us know a new contact within your company to send the bulletin to.

If you have any sister companies or businesses you work closely with who you think would benefit from this bulletin (check with them first) then please let us know.

If you no longer wish to receive this bulletin then please let us know at NorthEastCrimeReduction@Scotland.pnn.police.uk

URGENT MESSAGES WILL BE SENT OUT AS APPROPRIATE

Crime Reduction Unit
North East Division

Email: NorthEastCrimeReduction@scotland.pnn.police.uk
Website: www.scotland.police.uk
Twitter: www.twitter.com/NorthEPolice
Facebook: www.facebook.com/NorthEastPoliceDivision

Police Scotland's North East Division covers rural and urban areas in Moray, Aberdeenshire and Aberdeen City. The division has five territorial command areas which have their own dedicated Area Commander, who is responsible for the daily policing function. Each command area is served by a number of community policing teams whose activities are built around the needs of the local community. These teams respond to local calls and look for long term solutions to key issues. They are assisted by the division's Crime Reduction Unit who deliver against Force and local priorities in a number of areas, including physical and social crime prevention, supporting and enhancing community engagement and creating and sustaining strong and effective partnership working