CLEVELAND POLICE

Cyber Crime Newsletter

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

WARNING: National Insurance scam leads to surge in calls to Action Fraud ALERT 22-01-2021

Action Fraud, the national reporting centre for fraud and cyber crime, is warning the public about a National Insurance scam, after it received over 1,000 extra calls from members of the public this week.

Victims have reported receiving an automated telephone call telling them their "National Insurance number has been compromised" and in order to fix this and get a new number, the victim needs to "press 1 on their handset to be connected to the caller".

Once connected to the "caller", victims are pressured into giving over their personal details in order to receive a new National Insurance number. In reality, they've been connected to a criminal who can now use their personal details to commit fraud.

Pauline Smith, Head of Action Fraud, said:

"We are asking the public to remain vigilant and be cautious of any automated calls they receive mentioning their National Insurance number becoming compromised.

"It's important to remember if you're contacted out the blue by someone asking for your personal or financial details, this could be a scam.

"Even confirming personal details, such as your email address, date of birth or mother's maiden name, can be used by criminals to commit fraud. If you have any doubts about what is being asked of you, hang up the phone. No legitimate organisation will rush or pressure you."

How to protect yourself
If you receive an unexpected phone call, text message or email that asks for your personal or financial details, remember to:

STOP
Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE
Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT
If you have provided personal details to someone over the phone and you now believe this to be a scam, contact your bank, building society and credit card company immediately and report it to **Action Fraud** at www.actionfraud.police.uk or by calling **0300 123 2040**.

You can also contact CIFAS to apply for protective registration. This means extra checks will be carried out when a financial service, such as a loan, is applied for using your address and personal details, to verify it's you and not a fraudster.

For more information and guidance please visit: https://www.actionfraud.police.uk/news

---

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Coronavirus vaccine scams warning
ALERT 07-01-2021

Action Fraud is warning the public to remain vigilant as criminals begin to take advantage of the roll out of the COVID-19 vaccine to commit fraud.
As of 7 January 2021, Action Fraud, the national reporting centre for fraud and cyber crime, had received 57 reports in relation to the COVID-19 vaccine.

Pauline Smith, Head of Action Fraud, said:
"The vaccine is a crucial tool in fighting the coronavirus and keeping people safe. Thankfully, the number of reports into Action Fraud are relatively low but we have seen an increase in the last two months, particularly around scam text messages.

“Remember, the vaccine is only available on the NHS and is free of charge. The NHS will never ask you for details about your bank account or to pay for the vaccine. If you receive an email, text message or phone call purporting to be from the NHS and you are asked to provide financial details, this is a scam.”
Action Fraud has received reports from members of the public who have been sent text messages claiming to be from the NHS, offering them the opportunity to sign up for the vaccine. The texts ask the recipient to click on a link which takes them to an online form where they are prompted to input personal and financial details. In some cases the online form has looked very similar to the real NHS website.

How to protect yourself:

In the UK, coronavirus vaccines will only be available via the National Health Services of England, Northern Ireland, Wales and Scotland. You can be contacted by the NHS, your employer, a GP surgery or pharmacy local to you, to receive your vaccine. Remember, the vaccine is **free of charge.** At no point will you be asked to pay.

- The NHS will never ask you for your bank account or card details.
- The NHS will never ask you for your PIN or banking password.
- The NHS will never arrive unannounced at your home to administer the vaccine.
- The NHS will never ask you to prove your identity by sending copies of personal documents such as your passport, driving licence, bills or pay slips.

If you receive a call you believe to be fraudulent, hang up. If you are suspicious about an email you have received, forward it to report@phishing.gov.uk. Suspicious text messages should be forwarded to the number 7726 which is free of charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by calling 0300 123 2040 or visiting www.actionfraud.police.uk.

For more information and guidance please visit: https://www.actionfraud.police.uk/news

---

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Action Fraud warns of new courier fraud tactic after receiving 120 reports in 24 hours

ALERT 18-12-2020

New alert from Action Fraud and the National Fraud Intelligence Bureau (NFIB) about courier fraud.

In the past 24 hours, Action Fraud has received 120 reports of courier fraud. Victims have reported a particular tactic of being called by someone impersonating a police officer. The

suspect uses the name Eric Shaw and gives over his badge number, in order to appear trustworthy to victims.
The suspect asks victims to move money to a “secure bank account” until the victims are sent a new national insurance number. In reality, their money is being transferred into an account under the criminal’s control.

What is courier fraud?
Courier fraud is when victims receive a phone call from a criminal, pretending to be a police officer or bank official. Typically, victims are told to withdraw a sum of money and someone is sent to their home address to collect it. Criminals may also convince the victim to transfer money to a ‘secure’ bank account, hand over their bank cards, or high value items, such as jewellery, watches and gold (coins or bullion).

How to protect yourself and your loved ones:

- Your bank or the police will never call you to ask you to verify your personal details or PIN by phone, or offer to pick up your bank card by courier. Hang up immediately if you receive a call like this.
- If you need to contact your bank back to check the call was legitimate, wait five minutes; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to contact your bank.
- Your debit or credit card is yours: don’t let a stranger take it from you. You should only ever have to hand it over at your bank. If it’s cancelled or expired, you should destroy it yourself.

Spot the tell-tale signs:

- Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity, but is asking you for personal information, or even your PIN, to verify who you are.
- They’re offering to call you back so you can be sure they’re genuine, but when you try to return the call, there’s no dial tone.
- They say they’re trying to offer you peace of mind by having somebody pick up the card for you, to save you the trouble of having to go to your bank or local police station.

If you think you’ve been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

For full details, please visit: www.actionfraud.police.uk and select ‘Newsroom’ followed by ‘News’

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Fake DPD messages lead to over £200,000 in losses since June
ALERT 17-12-2020

Action Fraud is warning the public to remain vigilant as victims report losing £242,000 to criminals purporting to be from parcel delivery company DPD since June.

In November alone, the Suspicious Email Reporting Service (SERS), a tool launched by the National Cyber Security Centre (NCSC) and the City of London Police earlier this year, received 5,478 reports of suspicious DPD emails. This is an increase of 655% when compared to the previous month.

Action Fraud has also received 166 reports of suspicious DPD text messages between June and November this year, with victims reporting a total loss of £139,000. A further 35 reports were made in the first week of December, with victims reporting a total loss of £103,000.
The messages purporting to be from DPD claims that the delivery driver was "unable to deliver your parcel today" as "you weren't in or there was no safe place to leave it". The message provides instructions on how arrange another delivery. The links in the messages lead to fraudulent websites that request a small payment to rearrange the delivery.

If the victim makes this payment, they'll receive a phone call within a few days from someone purporting to be from their bank to inform them about suspicious transactions on their account. Criminals carrying out this scam are able to use a tactic called 'spoofing' to make the call or text appear genuine by cloning the phone number, or sender ID, used by the bank.
The victim is informed that their bank account may be compromised and is instructed to transfer their money to what they believe is an alternative secure account to prevent further losses. In reality, their money is being transferred into an account under the criminal's control. In other cases, suspects have gained enough personal details and security information during the phone call with the unsuspecting victim, to enable them to take out a loan in the victim's name. The criminals then transfer the loan to an account under their control.

Pauline Smith, Head of Action Fraud, said:
"Phishing messages are commonly used by criminals to gain access to our personal and financial details, leaving them free to commit fraud and take your money.
"At this time of year people are often sending parcels and gifts to friends and family, especially this year with people not being able to meet up in the same way for Christmas. Criminals are relying on the fact that we may need to reschedule a delivery to make their communication seem genuine. This is why we're urging the public to follow some simple steps to ensure they have a #FraudFreeXmas this year. Remember, if something feels wrong then always question it."

A spokesperson for DPD, said:
"We are aware that there have been a number of fake DPD emails trying to get consumers to send money for parcels to be re-directed. We would never do this nor would we ask consumers to give us their bank details.
"There is an easy way to check the email is safe, only emails sent from one of three DPD email addresses are genuine. These are dpd.co.uk, dpdlocal.co.uk or dpdgroup.co.uk. Fake or scam emails are nearly always sent from a private email address and certainly not from an official

DPD one. Any other sender email address, especially if the email is asking for money is highly likely to be a scam email.
“We would encourage anyone who has received a fake email to report it to report@phishing.gov.uk.”

Always remember:

- Your bank, or other official organisations, will never ask you to share personal or financial information over the phone, or via text or email. If you need to check that it’s a genuine message, contact them directly.
- You can report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk.
- You can report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.

If you have acted upon a message you have received, and you think you may be a victim of a fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040 as soon as possible.

Keep up to date with Action Fraud news, please visit: www.actionfraud.police.uk and select ‘Newsroom’ followed by ‘News’. Alternatively you can follow Action Fraud Twitter account at https://twitter.com/actionfrauduk

---

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NEWSROOM

Over £2 million lost to criminals impersonating well-known broadband providers
ALERT 13-12-2020

New alert from Action Fraud and the National Fraud Intelligence Bureau (NFIB) about computer software service fraud.
2,007 reports of computer software service fraud were made to Action Fraud last month. Victims reported losing a total of £2,148,976. This is a 22% increase in reporting compared to the previous month.

Action Fraud has received reports of criminal’s cold calling victims purporting to be calling from well-known broadband providers primarily, claiming that the victim has a problem with their computer, router or internet. The suspect persuades the victim to download and connect via a Remote Access Tool (RAT), allowing the suspect to gain access to the victim’s computer or mobile phone. Some reports also state that criminals have been using browser popup windows to initiate contact with victims.

Victims are then persuaded to log into their online banking to receive a refund from the broadband provider as a form of compensation. This allows the suspect access to the victim's bank account, and the ability to move funds out of the victims account into a UK mule account. There has also been an increase in the variety of service providers being impersonated, with multiple providers being affected.

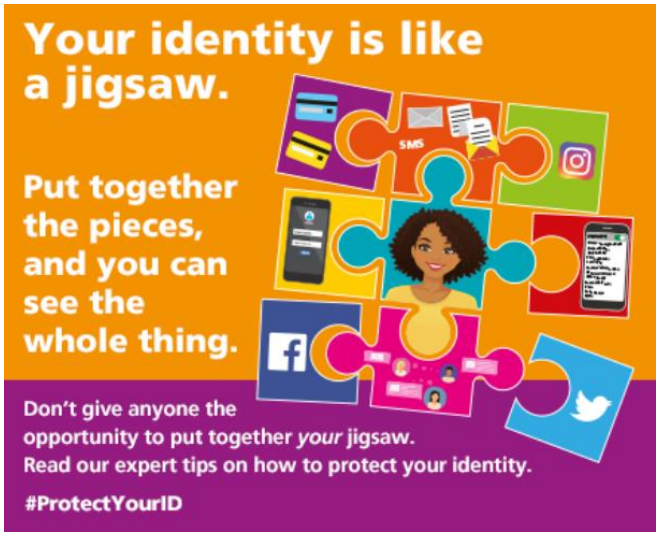
Always remember:

- Genuine organisations would never contact you out of the blue to ask for personal or financial details, such as your PIN or full banking password.
- Never install any software, or grant remote access to your computer, because of a cold call.
- Don't contact companies promoting tech support services via browser pop-ups.
- Hang up on any callers that claim they can get your money back for you.
- If you have made a payment, contact your bank immediately. They can help you prevent any further losses.
- If you granted remote access to your computer, seek technical support to remove any unwanted software. If you need tech advice, look for reviews online first or ask friends for recommendations.

If you think you've been a victim of fraud, report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

GET SAFE ONLINE Get Safe Online Free expert advice

Why is protecting your identity so vital?



Your identity is one of your most important possessions. It helps to prove that you're you, it enables you to verify your age online or in the pub, apply for a driving licence or a loan, get a mobile phone contract or a passport. And much, much more.

So when a cybercriminal steals your identity, they can do all of these things in your name too. As well as selling it on to other criminals and even committing criminal acts in your name.

Usually, identity thieves work online, looking for snippets of information about your life in social media posts and profiles, and unprotected email accounts. They exploit the fact that people like to share personal information with their online friends – and can be lax with security. Equally, they can find confidential information like National Insurance and bank account numbers in un-shredded rubbish.

It doesn't take many of these snippets for them to successfully steal your identity and wreak havoc with your life.

Get Safe Online have put together some expert tips to help you protect your identity.

- **Never share** account details or other information that you use to prove your identity, with friends, family or other people.
- **Think about what you share on social media**, such as date of birth and family members' or pets' names you also use in your passwords. Don't post details or images of your driver's licence, passport, NI number or other confidential items.
- **Never reveal private information** in response to an email, text, letter, phone call or web form unless you're certain that the request is authentic. Call to check, on the number you know to be correct.
- **Install the latest software, app and operating system updates** on your computer and mobile devices. Better still, set them to update automatically.
- **Make sure all your passwords are strong**, and keep them safe. Try using three random words, combined with capital and small letters, numerals and symbols. Don't use the same password for more than one account.
- **Use a strong and separate password** for your email accounts.
- **Don't connect to public Wi-Fi hotspots** when doing anything confidential online. They may not be secure, and they may even be fraudulent.
- **Always beware of people looking over your shoulder** when you're entering private information on a computer, mobile device or ATM.
- Arrange for **paperless bills and statements** instead of printed ones.
- **File sensitive documents securely**, and shred those you no longer need – preferably with a cross-cut shredder.
- **Get regular credit reports** to check if anybody has taken out finance in your name.

#ProtectYourID

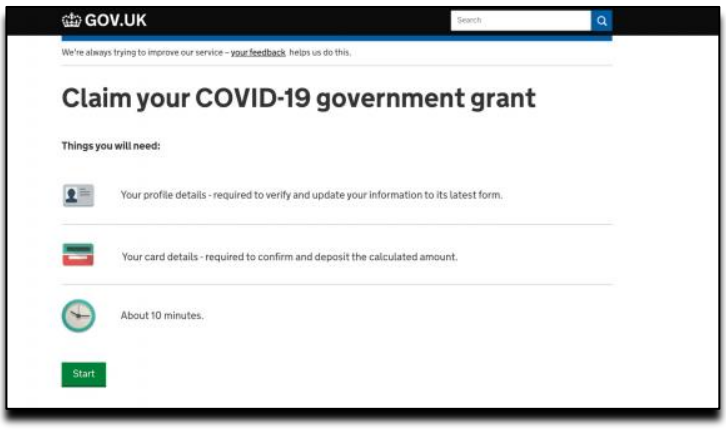
For full details, please visit: https://www.getsafeonline.org/protectyourid/

GET SAFE ONLINE .org Get Safe Online Free expert advice

NEWS

New 'HMRC' scam texts follow new lockdown

ALERT 05-01-2021



Scammers are already busy sending out fake 'HMRC' texts following yesterday's announcement of another national lockdown.

Frauds exploiting people's concern and confusion over COVID-19 began as soon as the pandemic hit, with numbers subsequently rocketing. The many themes have included fake test and trace calls to tax refunds, advertisements for non-existent PPE to vaccines, and fraudulent offers to deliver food and medical supplies in return for prepayment.

The latest scam text message also includes a number of variants, with one reading "From HMRC: The third lockdown has been announced, we have been issued a grant off *(sic)* £240 to help during this period, visit to claim:"
Clicking on the link takes the recipient to a fraudulent website (shown here), which impersonates the official gov.uk site. It tells users that they will need to have their card details ready.
Again, the latest tranche of scam messages includes those promising tax rebates.
Speaking to Sky News, an HMRC spokesperson said: *"Criminals are taking advantage of the package of measures announced by the government to support people and businesses affected by coronavirus.*

"Scammers text, email or phone taxpayers offering spurious financial support or tax refunds, sometimes threatening them with arrest if they don't immediately pay fictitious tax owed.
"HMRC has detected 275 COVID-19 related financial scams since March, most by text message. We have asked Internet Service Providers to take down 254 related scam pages," they added.
"Several of the scams mimic government messages as a way of appearing authentic and unthreatening.
"Over the last year HMRC reported 3,387 phone numbers being used in tax-related phone scams to telecommunication companies for takedown, and responded to over 306,219 reports of phone scams from the public, an increase of 47% on the previous year."

Any unsolicited texts, emails or phone calls claiming to be from HMRC offering financial assistance, informing you that you have either underpaid or overpaid tax or requesting your bank details, should be treated with suspicion.

Also, any website claiming to be an official government site should have the www.gov.uk address. (NHS sites' URL is www.nhs.uk).

The NCSC advises that suspicious text messages should be forwarded free of charge to 7726. If you discover that you have been the victim of COVID-related or any other type of fraud, report it to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

For full details, please visit: https://www.getsafeonline.org/news/

Net Aware | O2 | NSPCC Let's keep kids safe online

Let's keep kids safe online

NEWS

How to use parental controls on popular gaming devices
06-01-2021

With the introduction of new technologies, improved graphics and different ways we can connect (hello virtual reality), the gaming world is constantly evolving. And fast! While this creates new and exciting ways people can stay entertained, it also introduces new risks for young people who like to spend their time playing games online.
Not all games have safety settings, so when a child gets a new device, setting up parental controls is an important first step to help keep them safe. Check out our guide below for more information on how to set these up on popular devices.

What are parental controls?

Most games consoles have parental controls that can help you manage what your child does online and when. For example, some have settings that let you switch off communication features to stop your child talking to someone they don't know. Others let you set filters to stop your child from downloading games that might not be suitable for them.

How to set up parental controls on Microsoft Xbox

All Xbox consoles have a variety of features available for parents and carers to help keep their child safe. These can be set up either through the console or online with an Xbox Live account. Here are some of the settings we would recommend exploring.

Age restrictions – Set your child's age to stop them downloading games that might not be suitable.
Timer – You can set a timer to manage how much time your child spends playing.
Chat box – Switch off the chat function to stop your child from chatting with people they might not know.
Content filter – If switched on,
This will help stop your child seeing content they might find upsetting.
In- app purchases – Helps to stop your child from making in-app purchases.
To manage the parental controls on your child's device we would recommend setting up a **Family Group account** so they can't change them.

To set up parental controls on your child's console

1. Go to 'Settings' and select 'Family'.
2. Select your child's profile.
3. Under 'Privacy and online settings', select 'Change settings'.
4. Adjust the settings you would like to change and press 'Save'.

To set them up on a web browser

1. Sign into your **Xbox Live**
2. Select 'My Account'.
3. Select 'Security and Family Forums'.
4. Select 'Xbox 360 Online Safety' and choose the account you'd like to change.
5. Select 'Blocked' next to the areas you want to limit your child's access to.

Check out Microsoft's advice on **Gaming that is safe for all** for more information on the different settings available.

How to set up parental controls on a PlayStation device

To set up parental controls on a PlayStation console you need to set up your own PlayStation Network account and an account for your child. Once you've done this you'll be able to access these features to help manage how your child spends time gaming:

Timer – Helps to manage how much time your child spends on the console.
Spending limits – Set a maximum spend limit to stop your child from downloading too many paid games or purchasing in-app rewards.
Audio and text chat – Switch these off to stop unwanted contact from people your child might not know.
Age restrictions – Set age ratings so your child can't download certain games, films and TV shows.
Web browser – Prevents your child from using the web browser or stops them from accessing certain sites.
PlayStation VR – Helps you manage whether they're allowed to access this feature. Although, it's worth noting this is switched off by default for under 12s.

Just like on Xbox, you can set them up on a web browser or console.

To set up parental controls on your child's console
1) Go on your child's console.
2) Go to 'Settings'.
3) Select 'Parental Controls' and then 'Family Management'.
4) Choose the account you'd like to set controls for.

To set them up on a web browser
1) Sign into your PlayStation account.
2) Select 'Family Management'.
3) Choose the account you'd like to set controls for.
Check out **How to set parental controls and spending limits on PlayStation®4** for more information on how to set them up.

How to set up parental controls on Nintendo devices

Nintendo also has parental controls available to help keep your child safe on the device. To access these settings, you will need to set up a four-digit pin and they include:

Age rating limit –Stops your child downloading games that might not be suitable.
Web browser access - Limits access to web browser and news channel.
Communication features – Lets you manage which communication features your child can access or switch them off completely.
Manage shop – Lets you manage whether your child can download from the Wii Shop Chanel using Wii Points.

To adjust the parental control settings:
1) Go to 'System Settings' on the console.
2) Select the blue arrow.
3) Select 'Parental Controls' and select 'Yes'.
4) Enter your four-digit pin.
5) Explore other settings.
Check out **Nintendo's guide on Parental Controls** for more information.

Top tips

Parental controls are a very useful tool but it's also important to work with your child so they understand other ways they can keep safe online.

1. **Talk to them** - Regularly check in with your child about the apps, sites and games they're using.
2. **Don't feel pressured** – Just because everyone is playing it, it doesn't mean it is appropriate for your child.
3. **Stay in the know** - Be aware of the features that are available within games and apps. You can find advice on some of the more popular games and apps that kids use on our Net Aware reviews.
4. **Let them know they can come to you** - Make your child aware that they can always come to you if they are upset or if they have a question about something.
5. **Talk to them about Childline** - Ensure your child knows that they can always contact **Childline** if they need further support.

For full details, please visit www.net-aware.org.uk and select 'News and advice'

Internetmatters.org
NEWS

Socialising safely online
05-12-2020

Connecting and sharing online is a given as it offers access to the digital world at the touch of a button. And with 47% of 3-10-year-olds owning a mobile*, it's important to stay on top of who

and what they do when they are socialising online. Below we have recommended fun and child-friendly online-related social activities for under 12s.

Online social activities

Here are some social activities your family can do to keep your kids entertained and not feel as if they're missing out!

- Do art together. Why not let your kids FaceTime their friends? And at the same time, have both follow a drawing tutorial or challenge? You can find some drawing tutorials/challenges here and here.
- Play Heads Up! Like charades, it's an interactive app that can be downloaded by both parties. Players hold their phone up to their forehead, and the others give clues to help them guess from various categories.
- Social games and apps – there are many gaming apps and platforms for kids, such as Roblox. For more recommendations, check out our Top video games that children want to play article.
- Have a virtual hang out or party! You can use Zoom, FaceTime, Google Meet or Houseparty, just to name a few.
- Have a watch party! With watch parties, you can watch movies or shows online while chatting with friends and family all at the same time. Stuck on what to watch? Take a look at our recommended watch picks.
- Allow social media socialising. With screen time more likely to increase, it's important to realise kid's screen time will increase, although it's not necessarily a bad thing, ensure your child has a balanced digital diet. Additionally, we strongly recommend keeping an eye on who and what they engage with.

Online safety tips

- Talk to your kids about what they do online – do you know what they are doing online? Ask them who they interact with online and always mention for them to not to accept friend requests from strangers.
- If you are video-calling, ensure you either review or set up privacy and security settings on the device beforehand. Check out our parental controls where you'll find various settings for different platforms, apps and devices.
- Teach them to limit what they share, i.e., their personal details such as their full name, school, address, family/friend information, etc. Use a safe screen name.
- Ensure yourself and your kids know how to block, mute or report on different platforms.
- Remind kids that once they post something online, they can't take it back. Even if the info is deleted from a site, you have little to no control over older versions that may exist on other people's computers and may circulate online.
- Review your kids' friends' lists regularly – you may want to limit their friends' list to only people you/they know
- Create a digital agreement to set some digital rules about tech use in and out of the home.

**Research by Super Awesome, extensive desk research and data from Insights People's Data Portal 2020*

For full details, please visit www.internetmatters.org and select 'News and opinion'

National Cyber Security Centre

NEWS

Public urged to secure second-hand devices ahead of January sales
28-12-2020

The NCSC has published guidance to help the public secure second hand devices.

- The National Cyber Security Centre (NCSC) issues first ever guidance for consumers buying or selling second-hand internet connected devices
- Transactions involving pre-owned tech expected to increase in the weeks immediately following the festive period
- Shoppers urged to consider guidance carefully when thinking about buying or selling used devices to ensure their personal data is not accessed by criminals

People looking to buy and sell second-hand tech devices in the post-Christmas sales are being urged to follow new guidance to protect them from having valuable data such as bank details stolen by cyber criminals.

The brand-new Buying and Selling Second-Hand Devices guidance published today (Friday) by the National Cyber Security Centre (NCSC) – a part of GCHQ – outlines the steps people can take to protect their personal data when buying or selling used tech.

Traditionally, the post-Christmas and New Year period sees a rise in the number of people selling their second-hand devices, such as mobile phones and tablets, as they have been replaced by newer versions over the festive season.
These devices – especially smartphones – contain more work, personal, and financial data than ever before, and this guidance highlights the importance of erasing this before selling so that it does not inadvertently fall into the hands of criminals.

The NCSC is also encouraging shoppers who buy a second-hand device to familiarise themselves with advice from the government's Cyber Aware campaign, which encourages users to ensure their devices are kept up to date and to turn on two-factor authentication on their online accounts.

Sarah Lyons, NCSC Deputy Director for Economy and Society, said:
"At this time of year many of us take advantage of the pre-owned tech market, either to grab a bargain or cash in on a device we no longer need.
"We want consumers to make the most of this market, but we also want them to be aware of the risks around security and personal data and what they can do to protect themselves.
"As people look towards the post-Christmas sales we would encourage them to follow the steps in our 'Buying and Selling Second-hand Devices' to help them stay secure and shop with confidence."

The advice, which can be found in full on the NCSC's website, includes tips on
- what to do before you erase the data on your device;
- how to erase the data on your device;
- choosing a second-hand device, and;
- Things to know before using a second-hand device.

Kate Bevan, Which? Computing Editor, said:
"Our research has found significant numbers of smart devices are being resold, but are no longer supported with security updates from manufacturers, leaving users vulnerable to hackers.
"Anyone considering buying a second-hand device should find out when it was released and check if the manufacturer is still providing updates before parting with their cash.
"As the secondary and refurbished market continues to grow for tech products, manufacturers must be more transparent about the lifespan of devices and how long they'll provide security updates for, so people can make clear decisions and aren't at risk of buying unsupported devices."

Earlier this year, the NCSC and the City of London Police launched the Suspicious Email Reporting Service (SERS), which received 2.3 million reports from the public in its first four months resulting in thousands of malicious websites being taken down. Members of the public

who have received a suspicious-looking email over the holiday period should forward it to **report@phishing.gov.uk**.

More advice on protecting yourself and your family online can be found by visiting the government's Cyber Aware website, which details six practical steps that help protect against the majority of common cyber threats.

For details, please visit - https://www.ncsc.gov.uk and select **News**

Weekly Threat Report 15th January 2021

Vigilance urged following COVID-19 vaccine scams

Cyber criminals are attempting to scam the public by taking advantage of the COVID-19 vaccine roll-out.

Action Fraud had received 57 reports regarding vaccine scams as of the 7th January and want to raise awareness. The scam comes in the form of email or SMS and uses the lure of being vaccinated by tricking victims into sharing personal and financial details - some of the scams even use forms that look very similar to those used by the NHS.

It's important to remember:

- The vaccine is completely free of charge.
- The NHS will **never** ask you for your bank account or card details.
- The NHS will **never** ask you for your PIN or banking password.
- The NHS will **never** arrive unannounced at your home to administer the vaccine.
- The NHS will **never** ask you to prove your identity by sending copies of personal documents such as your passport, driving license, bills or pay slips.

If you believe you have received a scam email regarding the vaccine, then you can report it directly to the NCSC using the Suspicious Email Reporting Service (SERS) by forwarding the email to report@phishing.gov.uk.

If you have received a suspicious text message then you can forward this to 7726. This free-of-charge service allows an investigation to take place and take action, if found to be malicious.

The NCSC has published advice on how to deal with suspicious phone calls, messages and emails.

Capcom releases new update on ransomware attack

An internal review conducted by Capcom shows that potentially up to 390,000 people could have had personal information stolen in last year's ransomware attack.

The Capcom review of the incident has revealed that credit card details were not part of the stolen information obtained by hackers.

Capcom are working with authorities to identify if any further personal information has been taken and have enlisted the help of, and as yet, unnamed Major IT security Specialist Company, to help investigate the intrusion and proactively prevent future attacks.

The NCSC has guidance for organisations on mitigating malware and ransomware attacks and for personal information being lost in breaches that can lead to phishing attacks.

Billions in Bitcoin residing in inaccessible wallets

A programmer in the US has lost the password to a hard drive which holds a digital wallet containing approximately $220 million in Bitcoin. He has a couple of attempts at accessing the hard drive left before he is permanently locked out.

One company reports that over $140 billion in the Bitcoin cryptocurrency is currently lost or inaccessible. Hard drive disposal and reformatting have both been cited in other cases of lost cryptocurrency fortunes.

Passwords are the keys to your online life. The NCSC has produced guidance on choosing secure passwords by using 3 random words, implementing two factor authentication (2FA) to further protect your accounts and storing them securely using your browser or a password manager. Writing passwords down on paper is also fine, despite the problem here, but any that you write down should be carefully looked after.

Sports clubs gather for summit on cyber security

Professional sports teams and national governing bodies have been coached on how to defend against the threat of cyber criminals.

On Wednesday (13 January), the NCSC hosted the first-ever cyber security summit for over 180 representatives from a range of clubs and organisations, including 11 Premier League and 35 EFL football teams, rugby clubs, and cricket clubs.

The virtual meeting highlighted the NCSC's recent Cyber Threat to the Sports Sector report, which revealed cyber criminal activity including an attempt to sabotage a transfer deal worth £1m involving a Premier League team.

The sports industry is a high-value target, with at least 70% of institutions suffering a cyber incident every 12 months, more than double the average for UK businesses.

Weekly Threat Report 8th January 2021

HMRC warn of COVID-19 scam text messages

Cyber criminals are continuing to exploit COVID-19 concerns - this time with scam text messages about a non-existent government grant.

The message offers the prospect of financial support as the UK moves into another lockdown, but no such grant exists and HMRC has warned people to be vigilant to this threat.

The phishing scam takes the victim to a fake website masquerading as GOV.UK which asks for financial information. A number of spelling and grammatical mistakes in the message give a clue that it is a scam.

It's important to know that HMRC will never offer a tax refund by text, email or phone. HMRC have issued some advice for those concerned about this particular scam.

275 HMRC-related scams have been uncovered since March with HMRC taking action against 254 scam webpages. They have also responded to more than 300,000 reports of phone scams from the public.

The NCSC has also published advice on how to spot and deal with suspicious text messages, emails and phone calls. Don't forget that you can also report phishing emails direct to the NCSC using the Suspicious Email Reporting Service (SERS).

Suspicious text messages can also be sent to Ofcom on 7726 for free.

PPE company's operations disrupted by former employee

Before leaving the PPE Company that employed him, a disgruntled Vice President created a fake staff account.

The medical equipment packaging company revoked his legitimate staff accounts, but the ex-employee used his fake account to damage over 100,000 company records - which took months to fix.
He was jailed for a year and a day and ordered to pay over $220,000 in reparation.

Organisations should ensure that they have good logging and monitoring processes in place to establish patterns of normal activity so that indicators of compromise can be identified, and if the worst happens, help identify the source and extent of the compromise.

The NCSC has produced some help on logging through our Logging Made Easy project. Our Cyber Security Design principles can also assist when setting up networks, as can the system administration guidance help in implementing a strategy to protect the most sensitive data.
There is additional advice on logging and monitoring in the Mobile Device Guidance.
The Centre for the Protection of National Infrastructure (CPNI) has also produced some guidance on managing the insider threat. https://www.cpni.gov.uk/insider-threat and https://www.cpni.gov.uk/reducing-insider-risk.

Hackney council cyber attack update

Cyber criminals have published documents on the dark web that they claim were stolen from Hackney Council in a cyber attack.

In a statement published on hackney.gov.uk, the council said it understands that the vast majority of sensitive and personal data it holds is unaffected. Concerned residents should contact the council's Data Protection Officer.

The NCSC has been providing support to the council and working with partners to understand the impact of this incident. The National Crime Agency (NCA) are coordinating the law enforcement response to this incident.
The NCSC has guidance available on how to effectively detect, respond to, and resolve cyber incidents.

Weekly Threat Report 18th December 2020

Guidance issued as SolarWinds compromised

SolarWinds, a popular IT system management platform has been compromised and could be used for further attacks on connected systems.

As a result of a cyber attack of their systems, an attacker was able to add a malicious modification to SolarWinds Orion products which allows them to send administrator-level commands to any affected installation. This modification causes the Orion products to connect to an attacker-controlled server to request instructions and does not rely on the attacker being able to directly connect from the internet to the Orion server.

Not all customers who have an installation with the unauthorised, malicious modification will have been seriously affected, but all should take immediate action.

The NCSC has been working closely with international partners as well as FireEye - a cyber security organisation who discovered the compromise. In a statement issued earlier this week, we recommended that organisations ensure any affected instances of SolarWinds Orion are installed behind firewalls disabling internet access (both outbound and inbound) for the instances.

The NCSC has now also published full guidance highlighting immediate actions for all organisations using the SolarWinds Orion suite of IT management tools.

We would also recommend further reading:

- SolarWinds have published a security advisory on this incident including details of affected software and the vendor's advice.
- FireEye has published a blog on its investigation. This includes extensive technical details which may help in investigation of a suspected server compromise.
- Microsoft has also published a blog on this attack which includes other potential routes for investigation of compromise.

Spotify reset passwords following data breach

Users of the music streaming platform, Spotify, may have had their passwords reset after personal data was exposed to a third party businesses.

Spotify admitted to the breach in a notification to US officials and confirmed that a vulnerability in their systems had now been fixed. The issue had been in place since April with it only being discovered last month.

Personal details such as date of birth, email addresses, gender and passwords may have been affected. Passwords have been reset for affected customers.

Spotify were also recently alerted to a leaky database by cyber security researchers containing logins for up to 350,000 users which could have been part of a credential stuffing campaign.

Data breaches can sometimes lead to your information being used for phishing scams. The NCSC has published advice on how to deal with suspicious phone calls, emails and text messages. You can even report suspicious emails to the NCSC directly.

If you're a Spotify user who has had their password reset then you might want to consider following the NCSC's Cyber Aware advice for creating strong passwords.

TAKE FIVE

Take Five is a national campaign offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

STOP	CHALLENGE	PROTECT
Taking a moment to stop and think before parting with your money or information could keep you safe	Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.	Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud

STOP AND THINK

1. Never disclose security details, such as your PIN or full banking password
2. Don't assume an email, text of phone call is authentic
3. Don't be rushed – a genuine organisation won't mind waiting
4. Listen to your instincts – you know if something doesn't feel right
5. Stay in control – don't panic and make a decision you'll regret

For further details visit www.takefive-stopfraud.org.uk

Cleveland Police **Cyber Crime Team** has welcomed a new member of staff, **Kelly Close** in the role of Protect Officer.

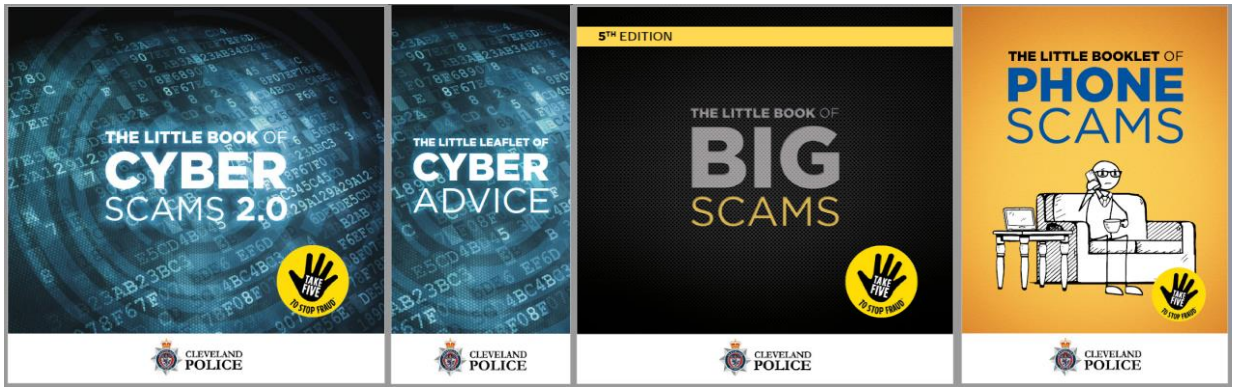
The role involves working with the public, organisations and businesses to safeguard themselves around cyber security.
More and more of us are using the internet in our everyday routines which can leave us more vulnerable.

We are able to offer free cybercrime awareness training to businesses in the Cleveland area. This is bespoke training to your company no matter the size or number of staff. For more information please contact cyber.crime@cleveland.pnn.police.uk

Information in this newsletter has been collated from following online sources;
www.actionfraud.police.uk
www.getsafeonline.org
www.net-aware.org.uk/
www.internetmatters.org
www.ncsc.gov.uk
www.takefive-stopfraud.org.uk

Should you become a victim of online crime please contact your local force on **101.** You can also report via **Action Fraud** using their online fraud reporting tool at **www.actionfraud.police.uk.**
Alternatively you can report to **Action Fraud** and get advice by calling **0300 1230 2040.**

Cleveland Police are dedicated to working with you to reduce vulnerability to fraud, and to protect you from harm. We are pleased to offer you the **Little Book Series**.



The booklets will help you to identify frauds and give you advice on how to best protect yourself and how to make a report.

If you would like a copy please email the Cyber Crime Team email address below and we will send you a PDF copy via email or through the post.
Alternatively you can access the booklets by visiting the Cleveland Police website via the following links/ QR Codes

Booklet Title	Website Link	QR Code
The Little Book of Cyber Scams and **The Little Leaflet of Cyber Advice**	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/	

The Little Book of Big Scams	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/prevent-personal-fraud/	
The Little Book of Phone Scams	https://www.cleveland.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/internet-email-mobile-fraud/	

If you would like to be added to the mailing list to receive this monthly newsletter or if you have any queries and would like further details on any of the above please contact:

Cyber Crime Unit
Cleveland Police

cyber.crime@cleveland.pnn.police.uk

Middlesbrough Police Office | Bridge Street West | Middlesbrough | TS2 1AB
Website | Facebook | Twitter | Instagram | LinkedIn

CLEVELAND POLICE

Public Service Transparency Impartiality Integrity

"Delivering outstanding policing for our communities"