Southern Internal Audit Partnership
Counter Fraud Unit

Fraud Bulletin No. 1

Southern Internal Audit Partnership provide a wide range of counter fraud services across a variety of public sector organisations.

THE BULLETIN

The bulletin covers the queries received by the Counter Fraud Unit and scams we have been notified of within the past few months. There is a definite trend of fraudsters exploiting the changes to how we work, the uncertainty, and peoples' feelings of vulnerability, coming from Covid.
We hope you find it helpful.

COUNTER FRAUD UNIT

We have a dedicated Counter Fraud Unit.
All staff are professionally accredited and we bring together significant experience of audit, and fraud prevention and investigation. We can also call upon specialists from the wider Partnership.

For more information on the services we provide please contact:
Iona Bond, Counter Fraud Manager
(iona.bond@hants.gov.uk)

General Advice

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. There are some things which we all need to remember.

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: Contact your bank immediately if you think you've fallen for a scam and also report it to Action Fraud.

The Impact of Covid

The pandemic has altered how we all live, and how and who we interact with. Criminals have used this to their advantage.

We continue to hear about online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived. There are also cases where fake testing kits have been offered for sale.

Criminals are also impersonating the Government to trick people. This includes using HMRC branding to make spurious offers of financial support through unsolicited emails, phone calls and text messages.

This situation is likely to continue, with criminals looking to exploit further consequences of the pandemic, such as financial concerns to ask for upfront fees for bogus loans, offering high-return investment scams, or targeting pensions.

Nick Barrett
Senior Counter Fraud Officer
Southern Internal Audit Partnership

December 2020

Southern Internal Audit Partnership
Counter Fraud Unit

Computer Software Service Fraud

Huge increases in the numbers working remotely mean that lots more people will be vulnerable to computer service fraud where criminals will try and convince you to provide access to your computer or divulge your logon details and passwords.

Never install any software, or grant remote access to your computer, as a result of a cold call.

Genuine organisations would never contact you out of the blue to ask for financial details such as your PIN or full banking password.

If you have made a payment inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.

If you granted remote access to your computer seek technical support to remove any unwanted software from your computer.

Don't contact companies promoting technical support services via browser pop-ups.

Mandate Fraud

This is where a fraudster sends in bank details to replace those used for a legitimate payment.

If you receive a request to move money into a new bank account, contact the supplier directly using established contact details, to verify and corroborate the payment request.

Establish robust internal processes for handling changes to payment details. For example, only designated employees should be able to make changes to payment arrangements.

Invoices, payment mandates, and other documents containing sensitive financial information should be stored securely and only be accessible to those staff that need them to perform their duties. Sensitive documents should be shredded before they are disposed of.

If you have made a payment inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.

Amazon Cold Calls

We have been alerted to several scams where fraudsters have been calling pretending to be from Amazon.

The first is from "Amazon Prime security" about a compromised Amazon account from which a series of payments have apparently been made. Having gained the person's trust, the fraudster instructs them to download remote access software, which is used to access the victim's online bank account.

A further scam starts with an automated telephone call where the victim will hear a recorded message alleging to be from Amazon Prime. The message advises the recipient that a scammer has set up an Amazon Prime account in their name and if they want to cancel it they should press '1'. The victim will then be connected to the fraudster who pretends to be an Amazon Customer Service representative who needs remote access to the computer to fix a security flaw to prevent this from happening again. The remote access will give them full view of the victim's personal information including online banking details.

Another variation is where an automated call says that Amazon Prime will auto-renew unless you press 1. This connects to the fraudster.

And finally, a school received a call from Amazon who had flagged suspicious spending over £1,000 on the school credit card. The call asked the school to respond to assist them to investigate. As the school does not have a credit card, they did not respond but did ask us to pass on a warning to others.

Southern Internal Audit Partnership
Counter Fraud Unit

Other Frauds to Watch For:

We have also noticed an increase in other types of fraud:

Breached home regulations scam
This is a fraudulent text message from .gov.uk issuing fines for leaving home

Free school meals scam
Which involves a fraudulent message to parents about 'free school meals' requesting bank details

CEO Fraud
With more people working at home, it is easier for fraudsters to impersonate senior decision makers, with seemingly valid reasons why they cannot be contacted. They request an emergency payment is made quickly and the normal controls are not followed.

Further Information

There is a wealth of advice and information available, useful links include

Scamsmart
ActionFraud
CIFAS
TakeFive
Citizens Advice
Trading Standards
and the National Cyber Security Centre.

Reporting to Action Fraud can be done online at https://www.actionfraud.police.uk or by calling 0300 123 2040.

To report offers of financial assistance from HMRC contact phishing@hmrc.gov.uk

Email scams can be forwarded to the newly established Suspicious Email Reporting Service https://www.ncsc.gov.uk/information/report-suspicious-emails