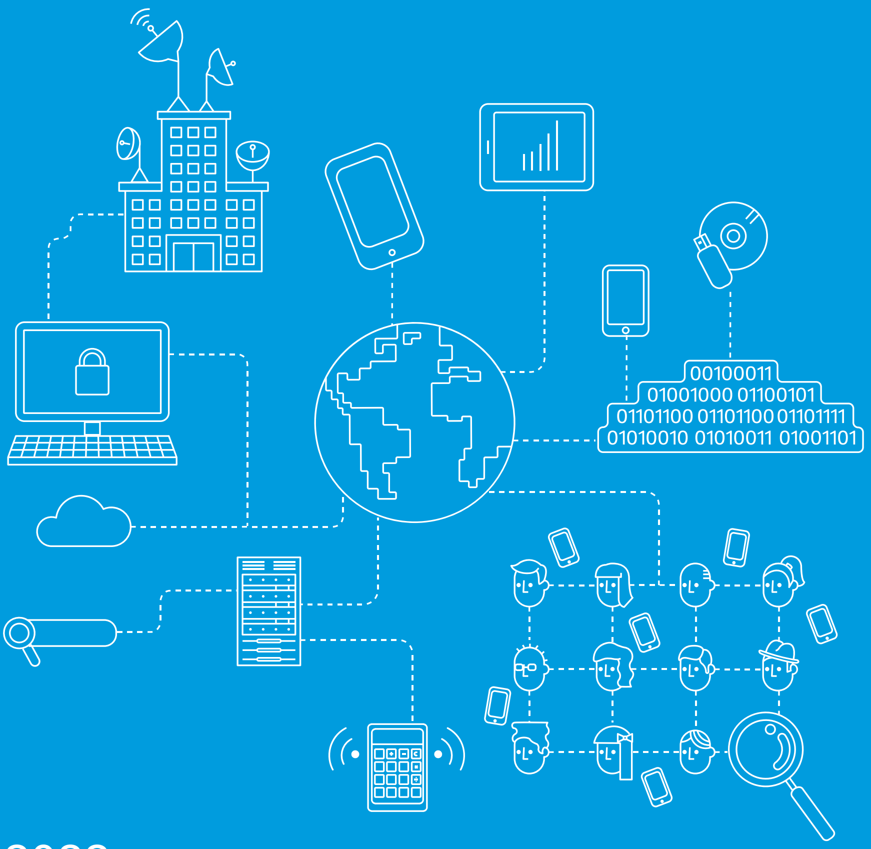
Being 'Scam Savvy' in the Cyber World



March 2022

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Contents

Being ‘scam savvy’ in the cyber world

Cyber crime is a serious threat to organisations. With many of us working online, to protect yourself and your organisation, it is more important than ever that you, as the first line of defence, are aware of scams.

Back in 2017, over a third of England’s NHS Trusts were disrupted by the global ransomware attack known as ‘WannaCry.’ This ‘worm’ exploited a vulnerability within the Windows operating systems and locked up the files, which could only be accessed through payment of a ransom in bitcoin. No NHS organisation paid the ransom but it is estimated that disruption to services cost the NHS around £92m. This could have been largely avoided, had many of the NHS victims kept up-to-date with security patches and this highlighted the importance of basic security practices.

Cyber criminals are firmly focused on the UK market. The past 12 months have seen the threat amplified by the coronavirus pandemic, as cyber criminals try to capitalise on the chaos. Our Cyber Security 2021 survey found that 20 per cent of organisations had experienced a cyber attack in the last 12 months, and 71 per cent of respondents said the attack was a direct result of the coronavirus pandemic.

95 per cent of cyber security breaches are due to human error, so user behaviour and education is the best way to protect your organisation against many of the most common scams.

In this document we highlight some of the scams we see across our NHS client base. We aim to equip you and your teams with the knowledge and training required to avoid scams and online fraud.

Topics covered in this document

- Invoice mandate fraud
- Salary payment diversion fraud
- Email interception
- Targeted phishing emails and fraudulent links
- Malware
- Password tips and best practice

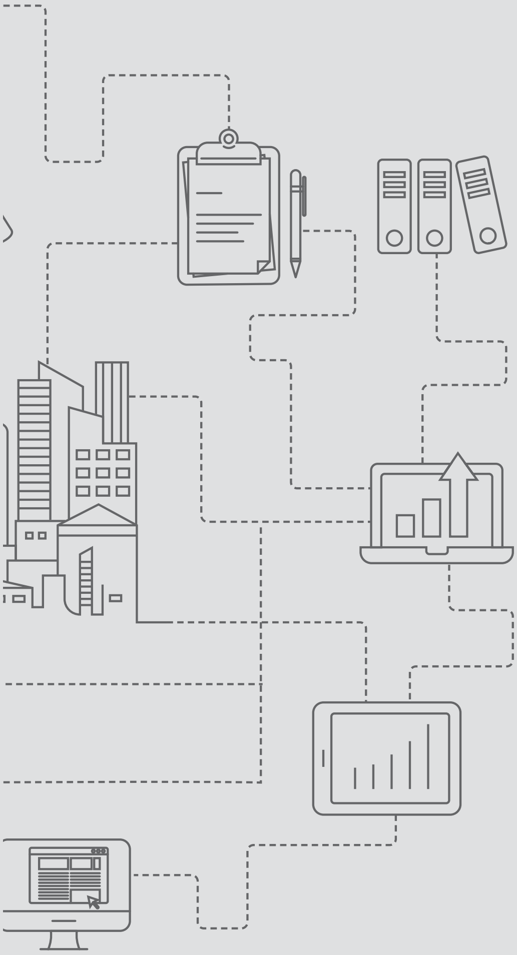
Invoice Mandate Fraud

In the NHS, payment diversion fraud is usually targeted at finance and procurement departments, in the form of mandate fraud. An initial email purporting to come from a known supplier is issued by a fraudster, requesting payments be made to a new bank account- which is controlled by the fraudster. The email address used can often be very similar in appearance to the genuine email account. If the change is made, any funds paid are lost to the fraudster.

Fraudsters have also approached this by initially requesting a change to the genuine supplier's phone number, ahead of making the request to change their bank mandate at a later date. This is in an attempt to pass the call back checks that should be conducted through known contacts.

ACTION TO TAKE

- **Raise awareness** of the different ways in which bank mandate fraud can be committed.
- **Verify requests to change mandate details verbally**, by contacting the company directly, using contact information already held on file and not shown on correspondence received.
- **Any requests for changes to a supplier's phone number must go through the same independent verification process**, as used with mandate change requests.
- **If you are suspicious about a request made by telephone, ask the caller if you can call them back and return the call using a number held on file.** Do not feel pressured to action the request, despite what the caller may say.
- **Pay close attention to email addresses used** for any subtle differences.
- **As well as bank account details, check wording used and logos used** on any invoices or paperwork received, against previous documents received that you know to be genuine.



Salary Payment Diversion Fraud

Payment diversion fraud is exactly what it sounds like. Typically, a link is emailed to an employee. The link often appears to be to their employer’s self-service login page but it is a spoof website set up by the fraudster. The spoof website records the employee’s username and password, and the fraudster uses this information to divert the employee’s salary payments into their own bank account.

These emails often use overly formal language and incentivise the employee to click the link, often with the ‘notification’ of a generous pay increase or an issue with their pay. For example:

> In accordance with the Fiscal Year 2021 Salary Allocation Guidelines (SAG) kindly be informed that your monthly salary starting January 2022 will reflect a 12.36 percent salary increase. Your new salary is analysed herewith. All documents are enclosed hereunder: view documents here.

> Your monthly salary starting from April 2022 will be raised by 13.84%. Enclosed is your salary increase letter. Download and keep a copy for your records. **when prompted, your date of birth on records must be authenticated**. View letter here.

> The payroll team has noticed some irregularities on your payslip and P60 form which may impact your January salary. Report is as attached. Kindly download and update accordingly as highlighted. **this is a secure document, hence authentication will be required**.

ACTION TO TAKE

- **Educate your teams** about the way you communicate salary increases and payroll issues, so that they are on the alert for such scam emails. It is very unlikely – or should be – that the first someone hears that they’ll be receiving a large pay rise is from an unsigned, impersonal email. Use multifactor authentication on self-service sites to strengthen access security by requiring more than one method to verify identity beyond the username and password.

- **Enable notification of change of bank account details** to ensure affected staff are aware of any changes and can report concerns at the earliest opportunity. Additionally, when it comes to approvals, ensure appropriate access rights and division of duties.

- **Run payroll reports to identify requests for bank details changes**. Doublecheck with the member of staff requesting the change. Check contact details and, if those have also been changed, use alternative sources of recorded contact details (email is not recommended).

- **Run IT reports on email addresses reported as phishing or blocked as spam** and check for malware on staff computers. There should also be anti-spoofing controls in place and filters/blocks on suspicious emails.

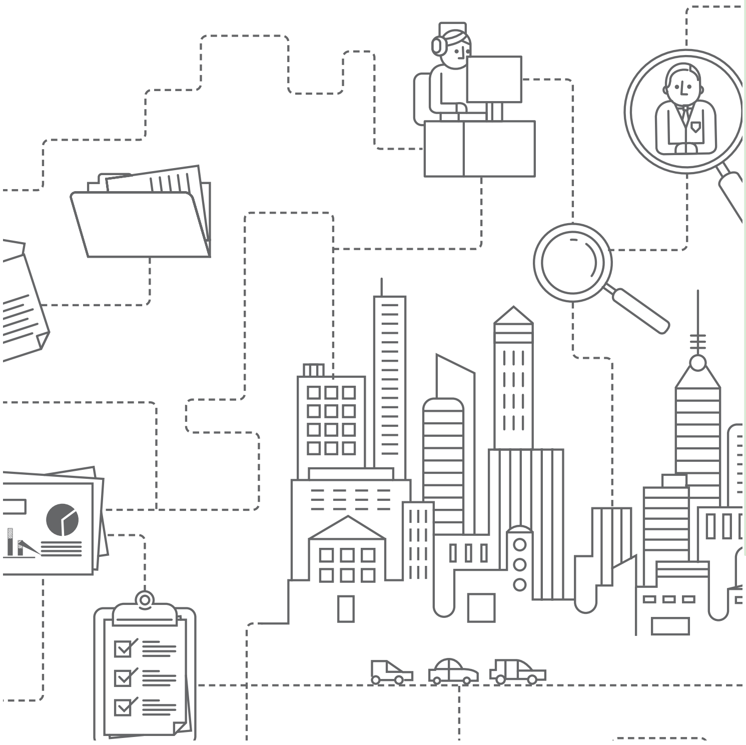
- **Review email accounts to check that all ‘rules’ applied are legitimate**. Some fraudsters have used employee email addresses to contact payroll directly and ask for changes to bank details. Through compromised email accounts, fraudsters have also set up ‘rules’ to divert certain emails – eg those containing the phrase ‘bank account’ – to accounts they control. The fraudster can then impersonate the employee to respond to verification emails from payroll and confirm changes to payment details.

Email Interception

Payment diversion fraud can also be achieved through email interception. Here, organised crime groups use viruses/malware to hack into suppliers’ email accounts, or those of key staff within the organisation (e.g. Finance Director, Head of Procurement, etc). This may be done through a phishing email to target a member of staff, spoofing a genuine email account or installing malware on a supplier’s devices. Fraudsters then intercept the email accounts and can make changes to the content requesting that future payments for products or services are made to a new bank account; or impressing a sense of urgency or authority, posing as a senior staff member to ensure that the change is made.

For example:

> Hi Phil, I have received this invoice from a supplier regarding an overdue invoice. Please can you pay this today.
> Connor Mann
> Director of Finance
> *Invoice attached*

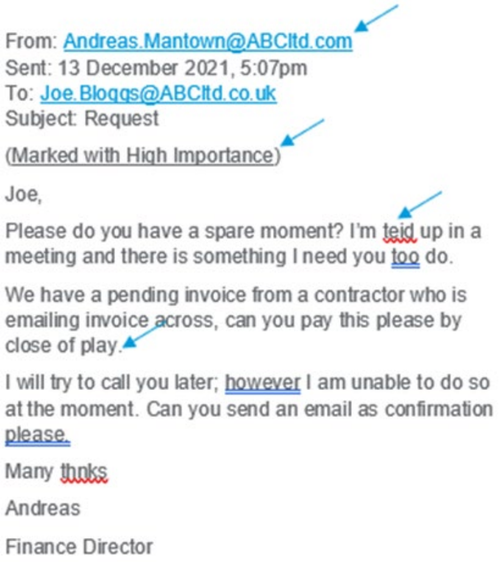


ACTION TO TAKE

- **Raise awareness** of the types of email interception fraud.
- **Communicate with your suppliers** the importance of keeping their operating systems up to date and secure to prevent phishing and hacking of email accounts.
- **Contact staff members directly**, using contact information already held on file, to verify any requests received.
- Organisations should **consider adding mitigation clauses in suppliers’ contracts regarding fraud losses** arising out of these types of incidents if the supplier is found to be in any way negligent.
- **Undertaking proactive audits** of suppliers where data or services are shared.
- **Ensure robust change of bank account request forms** (for example, request details of the last transaction made by the supplier) **and processes are in place** and, where bank accounts of concern are identified, organisations must immediately configure their finance systems to reject any them.
- **Use bank account verification software** to help reduce payment processing errors.
- **Use external data sources** to identify known accounts linked to fraudulent activity.
- **Bank statement checks** to look for any suspicious activity.
- **Contact your bank immediately** if any illegitimate payments have been made.
- **No PO no pay** can also highlight attempts of invoice fraud.

Phishing And Fraudulent Links

Spotting a targeted phishing email



From: Andreas.Mantown@ABCltd.com
Sent: 13 December 2021, 5:07pm
To: Joe.Bloggs@ABCltd.co.uk
Subject: Request
(Marked with High Importance)

Joe,

Please do you have a spare moment? I'm teid up in a meeting and there is something I need you too do.

We have a pending invoice from a contractor who is emailing invoice across, can you pay this please by close of play.

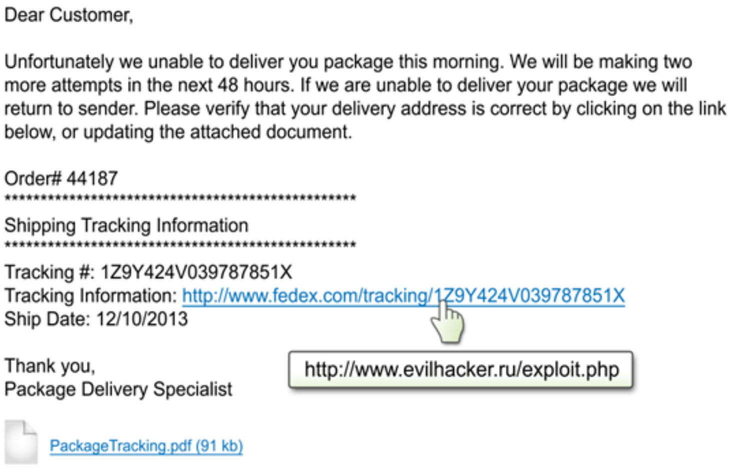
I will try to call you later; however I am unable to do so at the moment. Can you send an email as confirmation please.

Many thnks

Andreas

Finance Director

Identifying fraudulent links



Dear Customer,

Unfortunately we unable to deliver you package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 44187
****
Shipping Tracking Information
****
Tracking #: 1Z9Y424V039787851X
Tracking Information: http://www.fedex.com/tracking/1Z9Y424V039787851X
Ship Date: 12/10/2013

Thank you,
Package Delivery Specialist

http://www.evilhacker.ru/exploit.php

PackageTracking.pdf (91 kb)

Fake emails often display some of the following characteristics

- Spelling and grammatical errors
- Sender’s email address doesn’t correspond with the organisation’s website address.
- The email doesn’t use your proper name, but uses a generic greeting like ‘Dear Customer’ or ‘Hi friend.’
- Creates a sense of urgency: ‘act immediately or your account will be locked.’
- Prominent weblink, easily forged and looks similar, but check for character differences.
- A request for personal information such as username, password or bank details.
- You weren’t expecting to get an email from the company that appears to have sent it.
- The entire text of the email is an image rather than the usual text format.
- The image contains an embedded hyperlink that, if clicked, would divert to a bogus website.
- Double check the attachment file. Does it have an unfamiliar extension associated with malware such as .sip, .exe, .scr.

First Line of Defence

What to do if you get a suspicious email

ACTIONS TO TAKE

- Exercise **caution** when dealing with any unsolicited emails. Look carefully at spelling and grammar – poor spelling and bad grammar is unlikely to be from a genuine company.
- Check the **sender’s email domain** by hovering your mouse over the sender’s name.
- **Do not click on any links** in a suspicious email.
- **Do not reply to the email** or contact the senders in any way.
- **Do not open any attachments** or download content or images if you are prompted to do so.
- **Permanently delete** the email.
- **Apply the usual processes when making changes or payments.** Contact the organisation or person requesting the change using established contact details and verify the authenticity of the change. Do not make contact by replying to the email and do not respond using any of the contact details, such as phone numbers, shown in the email.
- **Immediately contact your IT security team** (or equivalent), and your bank if payment has been made.
- If you are a NHSMail user, you can **report it** using the ‘Report Phishing’ button or forward to spamreports@nhs.net.
- **Apply your Cyber Security Incident Response Plan** and raise awareness of the attempt amongst staff by way of issuing an alert.

Scams and phishing attempts are not always in the form of an email, but can be a text message, phone call or social media contact.
You can report all suspicious forms of contact to Action Fraud. If you have inadvertently clicked on a link or provided your details, advise the IT Security team at the earliest opportunity. If you have made payment and are concerned, you must contact the bank without delay as they can sometimes put a stop to the payment.

Passwords

SOME OF THE ACTIONS THAT CAN BE TAKEN

- **Avoid using predictable passwords**: Try to make sure that even somebody who knows you well couldn't guess your password in 20 attempts. A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27! or use a long and unique passphrase like We-Love-the-Summer-2022!
- **Only write down passwords in a secure location**, such as on a secure password manager programme – not near the device on a piece of paper.
- **Change** all passwords on a regular basis.
- **Do not share any of your passwords** with anyone else – if anyone else knows your password, it is no longer secure.
- **Switch on password protection**: Set a screen lock password, PIN, or other authentication method (such as fingerprint or face unlock).
- **Use two-factor authentication** (also known as 2FA) for any of your accounts where that option is available. It adds a lot of security for little extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method.
- Only use answers to **security questions** that are not available online/on social media accounts.
- **Only log into accounts from computers or devices that you trust.**
- **Consider extra security for highly privileged accounts** used by the organisation, IT and third parties.

For more information

For more information, please contact your IT Security team (or equivalent) and your Local Counter Fraud Specialist team:

Erin Sims

Associate Director and LCFS
T +44 07800 617456
erin.sims@rsmuk.com
erin.sims@nhs.net

Samantha Bostock

Senior Consultant and LCFS
T +44 07528 970373
samantha.bostock@rsmuk.com
samanthabostock@nhs.net

Tracey Revill

Counter Fraud Champion
fraudaware@staffsstoke.icb.nhs.uk

rsmuk.com

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are licensed by the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Whilst every effort has been made to ensure accuracy, information contained in this communication may not be comprehensive and recipients should not act upon it without seeking professional advice.