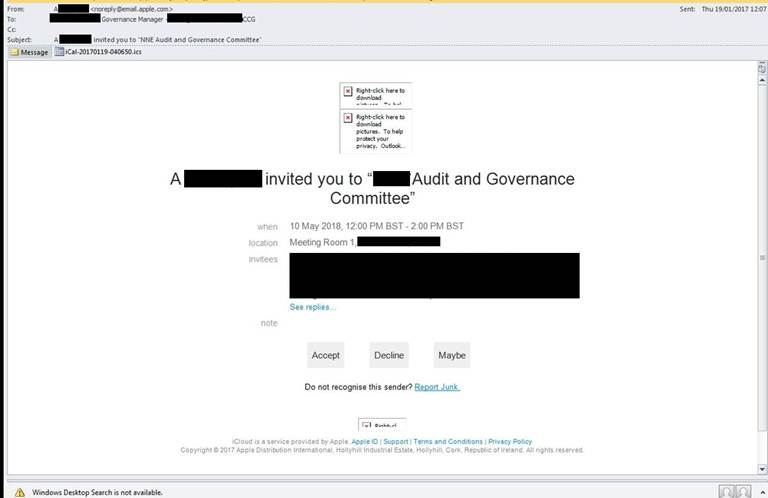
**Spam that is currently in circulation**

We have recently been made aware of suspicious meeting invites being sent to Audit and Governance Committee members at two of our client health bodies. At first glance the invites appeared to be sent from legitimate sources. On closer inspection the sender’s email address raised suspicions. It has since been confirmed that the emails were not sent by the committee member and are believed to be a scam.

The email address that was used on both occasions was [**noreply@email.apple.com**](mailto:noreply@email.apple.com). Both emails contained numerous links and a calendar attachment, each of which could contain malicious software or viruses. The name used as the sender/person inviting attendance of a committee meeting in each case was that of a genuine committee member.

Unfortunately scams of this sort, where distribution lists are used to send emails containing malicious content, appear to be on the rise. We would always advise against responding to emails that seem unusual / suspicious and further advise never to open links or attachments contained within them.

If you wish to clarify the legitimacy of any similar invites you receive please request this from your usual internal contact responsible for issuing committee invites, using previously known contact details.

The image below shows how these invites look.

**If you receive an email that is believed to be a fraudulent email here is a list of email addresses where you should send these emails:**

* UPS - [fraud@ups.com](mailto:fraud@ups.com)
* HMRC - [phishing@hmrc.gsi.gov.uk](mailto:phishing@hmrc.gsi.gov.uk)
* If you are suffering a live cyber-attack that is in progress, call now on 0300 123 2040 to report, do not report using the online tool. This service is available 24 hours a day, 7 days a week for businesses, charities and organisations. Our advisors are also available 24/7 on web chat if you have any questions.
* [phishing@hmrc.gsi.gov.uk](mailto:phishing@hmrc.gsi.gov.uk)
* [security.custcon@hmrc.gsi.gov.uk](mailto:security.custcon@hmrc.gsi.gov.uk)
* Santander bank - [phishing@santander.co.uk](javascript:location.href='mailto:'+String.fromCharCode(112,104,105,115,104,105,110,103,64,115,97,110,116,97,110,100,101,114,46,99,111,46,117,107)+'?subject=Phishing%20email&body=Thank%20you%20for%20the%20email%20you%20are%20about%20to%20send.%20Rest%20assured%20that%20we%20investigate%20each%20email%20we%20receive.%20However%2C%20due%20to%20the%20volumes%20we%20receive%20we're%20not%20always%20able%20to%20respond%20individually.')
* Barclays Bank – [internetsecurity@barclays.co.uk](mailto:internetsecurity@barclays.co.uk)
* Lloyds Bank – [emailscams@lloydsbanking.com](mailto:emailscams@lloydsbanking.com)
* RBS Bank – [phishing@rbs.co.uk](mailto:phishing@rbs.co.uk)
* TSB Bank – [emailscams@tsb.co.uk](mailto:emailscams@tsb.co.uk)
* NatWest – [phishing@natwest.com](mailto:phishing@natwest.com)
* [www.tradingstandards.gov.uk](http://www.tradingstandards.gov.uk/)
* Apple – [reportphishing@apple.com](mailto:reportphishing@apple.com)
* Gmail - <https://support.google.com/mail/answer/8253?hl=en>

**Derby Telegraph Article – Fraudulent Emails**

Police have issued a warning after a business in Derbyshire was targeted by a scam virus.

Officers said they have received reports of a strain of "ransom ware" called "Dharma" being circulated by fraudsters, which has affected a business in the county.

A spokesman for the force said: "Fraudsters will send an email to businesses containing an attachment. This attachment will contain ransom ware, that once downloaded will encrypt files and demand money to recover the files.

"The offenders utilising Dharma will not decrypt all files if the ransom is paid. They will decrypt a portion and then request further payment from the victim.

"We are urging victims to refuse to pay the ransom demands and to contact police and action fraud."

**Police have issued advice on how to stay safe online.**

**Police have not named the business concerned but they have issued the following tips to stay safe online:**

* Having virus protection is essential, ensure that it is kept up-to-date.
* 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 devices you back up to aren’t left connected to your computer as any malware infection could spread to that too.

The spokesman added: "If you, or anyone you know, have been affected by this fraud or any other scam, report it to Action Fraud by calling 0300 123 2040."

Read more at http://www.derbytelegraph.co.uk/police-warn-derbyshire-resident-of-new-dharma-scam-ransom/story-30115539-detail/story.html#1zl3yRICCY4jesbB.99

http://www.derbytelegraph.co.uk/police-warn-derbyshire-resident-of-new-dharma-scam-ransom/story-30115539-detail/story.html

**Advice on preventing telephone fraud**

GPC has been made aware that telephone systems used by practices may be vulnerable to fraudsters hacking into them and making premium rate calls. In one instance £2500 - £5000 of calls were placed over one weekend.

This is known as PBX/dial-through fraud, which occurs when hackers target Private Branch Exchanges (PBX) from the outside and use them to make a high volume of calls to premium rate or overseas numbers.

The victims are usually small to medium-sized businesses, but the National Fraud Intelligence Bureau has also noticed that a number of schools, charities and medical/dental practices being targeted where fraudsters are taking advantage of flaws in security systems.

This type of fraud is most likely to occur when organisations are most vulnerable i.e. during times when businesses are closed but their telephone systems are not, for example in the early hours of the morning or over a weekend or public holiday.

There are commercial organisations that will install software to prevent this and practices should consider whether this is a cost effective solution. However, a simpler alternative might be to place a block on international calls with the telephone system supplier.

This raises an issue of where, for example, a patient is hospitalised abroad and clinician to clinician communication is required, but the advice of GPC would be to ensure that an alternative mechanism for making and receiving such a call was in place, such as the mobile of one of the practice staff. Any cost to the individual could then be reimbursed.