nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

HOW TO PROTECT YOUR COUNCIL FROM CYBER-ATTACKS

Andy Hall, corporate account executive and cyber risk specialist at BHIB Insurance Brokers

Phishing emails – Tips to help protect your council

Phishing emails are one of the most common forms of cyber-attack, and as they become more sophisticated, the risk of your local (parish and town) council becoming a victim increases.

To help prevent this, the Cyber Insurance team at BHIB Councils Insurance has put together a list of quick and actionable tips below.

What is phishing?

Phishing is a cybercrime involving fraudsters reaching out to targets primarily via email but can also involve telephone calls or text messages. The cybercriminal will pose as a legitimate business or organisation to lure the target into providing sensitive information.

This usually includes requests for personally identifiable information, bank and credit card details and passwords. Although phishing attacks are becoming more sophisticated, there are some simple actions you can take to limit the risk of becoming a victim:

Check who the message is from

Vigilance is your primary weapon against phishing attacks, so always check who an email's sender is. It sounds simple, but it is very easy to forget to check – especially during a hectic day.

Look at the sender's email address closely; if you are unsure who they are, it is best to be over-cautious and not click on the embedded links or attachments within the email.

Check the addressee

It is common practice for legitimate emails to be personalised so that they will use your name, alias, or title. Suppose you receive an email from an individual or organisation that should know you but has a generic salutation such as 'Hi' or

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

'Good morning'. In that case, there is a chance it could be illegitimate and should be treated with caution.

Check the spelling and grammar

Phishing emails may come with poor spelling, often on purpose to avoid falling into spam or junk boxes. So, look for spelling and grammar mistakes like capital letters in the wrong place or a lack of punctuation.

Is the link URL genuine?

Something that might get overlooked is making sure the URL within the email that you are asked to click on is genuine and trustworthy.

Before you click, a valuable thing to do is to hover over the hyperlink so it displays the full link either in a pop-up box or in the bottom left of your email client. If the URL you see doesn't look legitimate, it is best not to click on it.

Are you being asked to 'act quick'?

Always be wary of any email or other communication asking you to respond or act quickly. Instructions such as 'click here immediately' or 'respond now' are common tactics cybercriminals use to create a sense of urgency and encourage you to click without checking.

Do not give any login details

Only give your login details to a trusted source or website you feel confident about or are familiar with. If you were to give this away, it could allow hackers access to your account, where they may be able to access further details, which could lead to a 'business email compromise attack'.

Report it!

The most important thing to do when you think you have received a suspicious email is to report it. If you feel you have fallen victim to a phishing attack, then the best thing to do is to say this to your IT department as soon as possible.

The sooner this is actioned, the more likely they will be able to help and reduce the possibility of this causing any damage or loss.

If you have received an email you're unsure about, you can also report it to the National Cyber Security Centre (NCSC) by forwarding it to report@phishing.gov.uk. The NCSC can investigate and remove scam email

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

addresses and websites. So, by reporting them, you can help reduce the number of scam emails being sent and protect others from becoming victims of cybercrime.

The key to avoiding phishing attacks is always to remain vigilant, as there is a chance that something can slip under the radar. It is also essential to ensure that all staff members, volunteers, and anyone else who may use your council's email network are fully aware of the risks of cybercrime and how to minimise the risk of becoming a victim of a phishing attack.

For more information on protecting your council from cybercrime, please email us at insurance@bhibcouncils.co.uk or visit www.bhibcouncils.co.uk.

Any views or opinions expressed in this briefing are for guidance only and are described in generic terms. They are not intended to substitute for appropriate professional advice relevant to individual circumstances. We have taken all reasonable steps to ensure the information contained herein is accurate at the time of writing. We would always encourage readers to seek specific professional advice.