CYBER SECURITY: HOW TO STAY SAFE

David Astwood, Technical Director at Microshade VSM, explains how local councils can stay safe in the virtual world.

Microshade VSM will be leading a webinar on Managing Your Cyber Security on 24th November - Check the events calendar for further details!

Town and parish councils are a popular and easy target for fraudsters, and email is increasingly being used to target officers and members.

Fraudsters tailor convincing emails designed to dupe unwary recipients. Councils are easy targets: inside information about council activities can be found from council website, minutes, multimedia sites, and lately from web meetings. Names and contact information for staff, officers and councillors are easy to find. Quite often, councils correspond with members of the public who are less security conscious or have insecure mailboxes which are easily hacked. All this gives fraudsters plenty of ammunition.

In June 2020, Microshade VSM became aware of an individual who was targeting councils by email. We know of five councils who have been targeted in the southwest. Emails were tailored to the council showing that the sender had researched the intended target - they appeared to come from the mayor or clerk, addressed the recipient personally, and contained nothing that a spam filter or recipient might find suspicious. "Can you do me a quick favour?" was all that one message said. If the recipient replied, the fraudster attempted to convince the target to make a payment to an account.

Apart from the current threat of impersonation, over 50% of all emails sent are spam, some just junk mail, but some with malicious payloads (viruses) or fraudulent content.

HOW TO STAY SAFE

Spam Filters

A good spam filter is essential and should intercept most inbound spam and impersonation attempts. Cloud-based spam and malware filters stop threats safely away from your own equipment.

A spam filter on outbound email can protect your reputation if your mailbox is hacked and can intercept outbound messages containing offensive language or content.

TIPS for Spotting Spam

- Check the sender's actual email address (if this is not visible, hover your mouse over or click on the sender's name)
- Be cautious if you don't know the sender
- Be suspicious of emails containing links, attachments, requests for payment or change of payment details, even if the email appears to come from someone you know. Always confirm new bank details with a telephone call
- Check the grammar and language used is consistent with the sender

Cyber Training

Even the best spam filter is never 100% effective (after all, spammers spend all their time trying to defeat them). It's also worth noting that 90% of data breaches over the last 2 years have been due to human error[1].

Provide your mailbox or IT users with training in how to spot fraudulent emails and stay safe online.

Computer Updates and Good Endpoint Security

To close vulnerabilities which hackers use to gain access to your computer, check that updates are running regularly. Uninstall any applications that you don't use. Keep remaining applications up to date.

Use independent online test websites to choose and install a good endpoint security product and make sure that it is kept up to date. This will protect you from malicious software and other threats. Products that come pre-installed on your new computer don't always perform well.

Cabinet Office Requirements for Public Sector Mailboxes

If you are a public body, the cabinet office requires that you put into place measures to keep your email system safe[2]. These include:

- Encryption so that emails cannot be read in transit
- Emails are stamped to ensure that the contents have not been tampered with
- Emails coming from your email addresses originate from your authorised email servers
- Emails not complying are appropriately disposed of, and you are informed

1 https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/ *2 https://www.gov.uk/guidance/securing-government-email*