WILTSHIRE FREEMASONS

Protecting Your e.mails

Many of our members will be aware of the scams used by unscrupulous people seeking to steal personal information. Your computer content is a prime target for such people, particularly individual email addresses. Very recently a Lodge member had their computer hacked and their email addresses hijacked. Within hours, members of the Lodge and the wider Province were being asked to 'help out the Brother who was *supposedly* suffering from laryngitis and needed some money transferred to a bank account' – of course it was a scam.

It is important that you protect yourself from an attack that attempts to steal your money, or your identity by getting you to reveal personal information - such as credit card numbers, bank information, or passwords. The best defence is awareness and knowing what to look for. Here are some ways to recognise an email that might be a scam.

Urgent call to action or threats: Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a friend or advisor who may warn you.

Tip: Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.

First time, infrequent senders, or senders marked [External]: While it's not unusual to receive an email from someone for the first time, this can be a sign of phishing. Slow down and take extra care at these times. When you get an email from somebody you don't recognise, or that Outlook or your computer identifies as a new sender, take a moment to examine it extra carefully using some of the measures below.

Spelling and bad grammar: Professional companies and organisations usually have an editorial and writing staff to make sure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.

Generic greetings: An organisation that works with you should know your name and these days it's easy to personalise an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.

Mismatched email domains: If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.

Suspicious links or unexpected attachments: If you suspect that an email message is a scam, don't open any links or attachments that you see.