SCAM EMAILS

A number of patients have reported receiving scam emails which refer to members of the surgery and their email addresses.

Neither the staff nor the practice would ask you for financial information or ask you to click a link regarding invoicing.

We are investigating the issues. However it is important that you take the following steps if you think you may have received a suspicious email.

1. Do not open emails or click on attachments/files that you are not expecting, especially requests that are urgent, ask for sensitive information or threaten a loss of access unless you comply with the contents.
2. Check suspicious emails with a phone call using a number from a trusted source not one on the email. Do not reply to the email.
3. Always use strong and unique passwords to enhance protection for your accounts.

If in doubt please do feel free to contact the practice to validate an email.