# Spam, Scam and Phishing email advice

U3A Stanway


If you regularly use email you are likely to be subject to receiving Spam, Scam and Phishing emails. These are generally fraudulent emails that are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

These include emails posing as being from 'trusted' sources such as your bank, HMRC or anywhere else that you have an online account. They may ask you to reveal personal details such as bank login, passwords and security phrases, or they may ask you to click on links that may take you to bogus websites or contain malicious software.

These types of email are all too common, but if you have a good antivirus and email system that has a good spam filter you will receive less of these types of emails, or they may be put straight into a "Junk" or "Spam" folder in your email account.

## How to spot spam, scam or "phishing" emails

The email can look as if it comes from a genuine source or email account. Look for the following warning signs:

- You don't know the sender.
- It will often contain incorrect spelling or grammar.
- The subject line and contents do not match.
- It may be addressed to "Dear Customer" instead of your actual name.
- The entire text of the email may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site.

It may also:

- Claim you are due a tax or bank charge refund.
- Claim there is a problem with your account or security that requires urgent attention.
- Ask you to update your password to avoid your account being suspended.
- Make an offer that seems too good to be true, such as investment opportunities, "get rich quick" and work from home schemes.
- Include an urgent offer end date (for example "Buy now and get 50% off").
- Ask you to forward the email to multiple people, and may offer money for doing so.
- Say you have a virus on your system that they can remove for you.
- Contain attachments or include links, either of which could install malicious software onto your PC, laptop, tablet or smartphone.
- Advertise online shopping, Viagra, pornography, dating or gambling services.
- Contain a (hoax) charity or money raising appeal.

## How spammers obtain your email address

- Using automated software to generate email addresses.
- Enticing people to enter their details on fraudulent websites.
- Hacking into legitimate websites to gather users' details.
- Buying email lists from other spammers.
- Inviting people to "unsubscribe" from bogus email marketing services.
- From names/addresses in an email cc line, or in the body of emails which have been forwarded and the previous participants have not been deleted.

The very act of replying to a spam email confirms to spammers that your email address exists, and can lead to further spam emails.

## How to Use Email Safely

- **Do not** open emails which you suspect as being scams.
- **Do not** respond to emails, open attachments or click on links from unknown sources.
- **Do not** forward emails which you suspect as being scams.
- If in doubt, contact (**by other means**) the person or organisation the email claims to have been sent by ... better safe than sorry.
- **Do not** make purchases or charity donations in response to email requests.
- **Don't** click on 'remove', "unsubscribe" or reply to unwanted email.
- When sending emails to multiple recipients, **list their addresses in the 'BCC'** (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving spam, scam or phishing emails.
- Similarly, **delete all addresses of previous parties in the email string**, before forwarding or replying.
- Most Microsoft and other email clients and internet security software come with spam filtering as standard. **Ensure yours is switched on.**
- Most spam and junk filters can be set to block emails from untrusted sources and allow email to be received from trusted sources, such as email addresses you add to your contacts list.
- When choosing an internet based (webmail) account such as Gmail, Hotmail and Yahoo! Mail, make sure you select one that includes spam filtering and that it remains switched on.

**Remember** to check junk mail folders regularly in case a legitimate email is posted there by mistake. **Delete** all other junk mail regularly.

For more information go to:

**Get Safe Online advice**

**Moneysavingexpert stop scam advice**

Prepared by: IT and Data Security Officer - Stanway U3A 16/4/2018