

# Don't take the bait with malicious email scams



Phishing emails appear to come from someone you trust, such as an online provider, bank, credit card company or popular website. These emails try to trick you into giving away sensitive information, such as your username, password or credit card details.

They may also try to install malware onto your computer by getting you to click a malicious link or open an infected attachment.

## Some general rules to follow:

### 1 Investigate Before You Click

Managers are unlikely to ask you to spend money, share sensitive emails (especially passwords) or pay invoices 'urgently' without picking up the phone.

### 2 Check The Sender

Is the email from support@silver-lining.com or slsupport123@gmail.com check the email as the later it's almost certainly fake.

### 3 Attachments From Unknown

Don't open attachments from unknown sources. Ask someone from your IT support desk to have a look if you are unsure, or better yet, delete the email.

### 4 Too Good to Be True

If its too good to be true it probably is. If you aren't expecting it, its probably not for you.

### 5 Before You Click

Hover over links to verify that links actual destination, even if the link comes from a trusted source.

### 6 Customer Email

The same logic applies to customers; if you receive an email from a customer from an unusual address, ignore it! – You can always follow up with a phone call or email their known address to confirm.

### 7 Internal/ External

Most companies have their email setup with a notification that sits at the top of an email and contains a warning if that email has been sent externally.

So if you get an email from a colleague or manager with the '**external**' warning, it's probably not from them.

### 8 Think Before You Act

Don't make decisions under duress, if an email says that you need to do something quickly and that time is of the utmost importance, it's a psychological trick!

If you receive an email that wants you to click a link or open a document, think 3 times about if you should proceed:

1. Do I know who it's from?
2. Am I sure that's who has actually sent it?
3. Is it something I would expect to receive?

03456 831 111 | [www.silver-lining.com](http://www.silver-lining.com) | [info@silver-lining.com](mailto:info@silver-lining.com)

