Email Safety Guidelines

Welcome to this training lesson on **Email Safety Guidelines.** In this lesson, we'll look at ways you can ensure you, your computer or device, and your personal information, remain safe.

Estimated Completion Time: 7 minutes.

Email Safety Guidelines

Introduction. One of the most useful tools in the modern world, Email is a means a lot of scammers and con artists will use in an attempt to trick you - trick you into giving them money, giving them your details, buying products that may not even exist, or installing a virus onto your device.

Let's have a look at some of the things you should watch out for to avoid falling for any of these scams.

Email Safety Guidelines

Your Email Software. You may be using any one of a number of popular email programs. Gmail, Yahoo, Outlook, Hotmail, are some of the common ones.

The popular programs, like those mentioned above, have, over the years, increased their security to ensure some level of safety. For example, they may block certain emails, or attachments in emails, or send others automatically to a spam folder.

But they are not perfect.

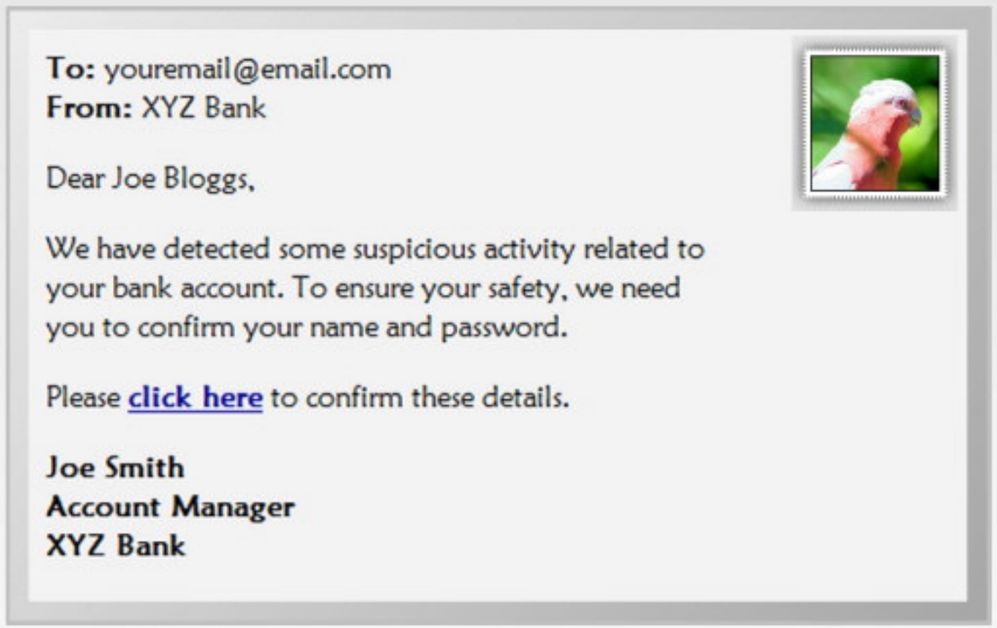
Email Safety Guidelines

Antivirus Software. If you are using anti-virus, or security software (and you should!), many of these programs will automatically link to your email program to provide an extra level of security. They can detect dangerous attachments, and other suspicious activity.

Many email programs may have their own virus scanning in use to help ensure any email attachments can be downloaded safely.

Email Safety Guidelines

Phishing Scams. Phishing scams are designed to get you to enter private, or sensitive information, or your passwords. A typical phishing scam email may appear to come from a bank, or from another company you may deal with, and may read something like this:



Banks and other institutions do not send emails like this. Do not follow the link, and do not enter your details. If you are concerned about your account, contact your bank or institution directly.

Email Safety Guidelines

Too Good to Be True. These scams lead to believe you've won the lottery. Or have been approved for credit. Or a beautiful model wants to contact you.

Bottom line - if it seems to good to be true, it is. Delete these emails. **Don't** follow or click on any links, and **do not** open any attachments that may be included with such emails.

Email Safety Guidelines

Requests for Money. Many of the too good to be true emails may come with a request for money.

Often, these emails will claim they can release some money for you - credit, or a lottery win, or some other windfall - if you can pay a small processing fee. Or provide your bank details.

Once again - don't fall for it. Delete these emails immediately, and if your email program allows it, mark them as spam.

Email Safety Guidelines

Fake Products. One of the most common email scams is the fake product. Scammers try to make a product sound attractive - and want you to buy it.

In almost all cases, these products do not do what they claim. Penis enlargements, super vitamins, credit cards, and all sorts of variations.

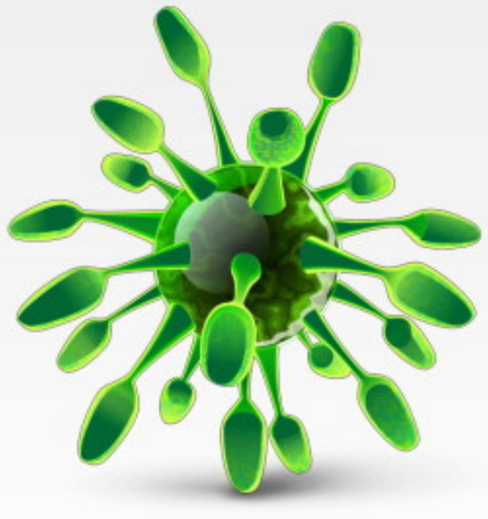
If you did not ask for the information, delete the email. Again, don't follow any links, don't open any attachments. And of course, do not buy the products.

Email Safety Guidelines

Dangerous Attachments. Dangerous attachments are executables, macros, or other program files included with an email that the email sender wants you to open.

Most email programs (or anti-virus software), these days, will block dangerous attachments. If you do receive such an email, and you do not know the person who sent you the email, **do not** open the attachment, no matter what it is.

Opening an attachment is one way scammers will be able to install a virus, trojan, or some other software to allow them to take control of, or take information from, your computer.



Email Safety Guidelines

Suspicious Links. Many scam emails will provide links that the sender wants you to click. It is quite possible that clicking on these links may take you to a website where malicious software may be installed on your computer.

As with the previous steps - if you don't know the person the link came from, do not open the links.

Don't be tempted. These sorts of emails will say all sorts of things to try and get you to follow the link.

Email Safety Guidelines

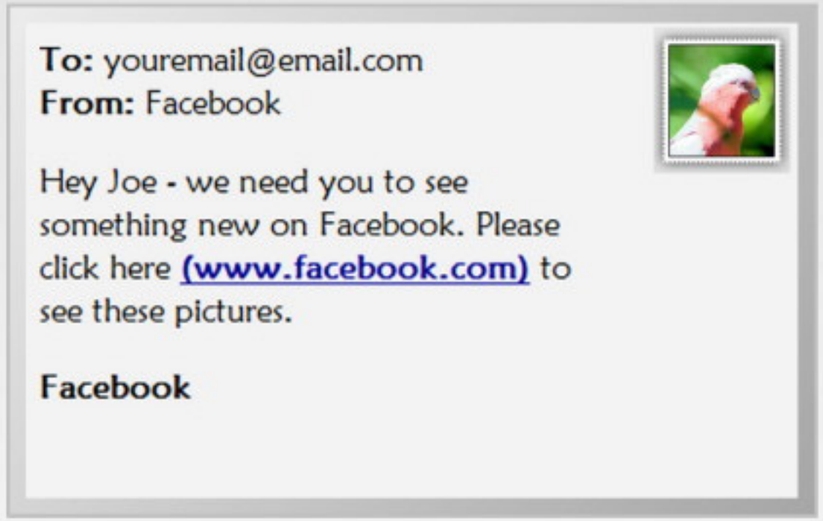
Fake Return Email Addresses. Sometimes, an email will appear to come from a valid address. For example, it may appear that the email comes from *customerservice@mycompany.com*. Sometimes, it may even appear to come from a friend.

It is **very important** to remember that this is **not necessarily** the email address that this email came from. Many email programs these days will spot such fraudulent behaviour, but it is not always possible.

If an email appears suspicious, do not reply to that email. If you need to contact that person or company, start a new email, and enter their email address manually (or from your address book).

Email Safety Guidelines

Fake Websites. Email can fake website addresses in two ways. First, a link may appear to link to one site, but actually link to another:



So - in the example above, the link may read **www.facebook.com,** but actually link to something completely different.

Or, it may attempt to fool you by linking to a website with a very similar website address - **www.faceboook.com,** for example. And this website, set up by scammers, may be set up to look very similar to **www.facebook.com.**

Email Safety Guidelines

Spam. Taken from an old Monty Python comedy skit, *Spam* refers to unsolicited bulk email. It is all too common, annoying, and in most cases, illegal.

If you think the email is from a reputable company, it should, by law in most regions, have an **unsubscribe** link you can use to remove your email address from their mailing list.

Email Safety Guidelines

Mark it as Spam. In the cases we've just discussed, we've recommended that you delete the email in question. However, if you get any suspicious email - or just an email you did not request - your email program will probably have a button or link marked **Report as Spam, Move to Spam,** or something similar, that you should use.

Using this feature will remove the email from your inbox, and it will also help your email provider determine in future - for yours and the benefit of other users - what emails are spam. It can then automatically redirect emails to your **Spam** folder if it is confident it is in fact unwanted spam.

Email Safety Guidelines

You've now completed this training lesson on **Email Safety Guidelines.** In this lesson, we looked at ways you can ensure you, your computer or device, and your personal information, remain safe.