The Silver Owl Network



Free ***Online Safety Guide***

No. 1
‘Email Scams’

It is estimated that nearly 1 million people in the UK have been victims of email scams (fraudulent emails). Getting caught by these emails can cost you money, take your time and cause unnecessary worry.

Criminals are increasingly targeting the older community in an effort to steal money and also personal details.

This FREE guide will help you identify which emails are potentially fraudulent, give you the information to deal with the emails (so you don’t get caught out) and also give advice on simple ways you can avoid problems with email scams in the future.

The Silver Owl Network

Index

The Silver Owl Network

Introduction

Technology has become part of our everyday lives.

From sending emails to catching up with the latest news or sport, the online world is never too far away.

But, there are people who want to use that technology to scam us, steal our personal information and make us worry about the safety of using emails and the internet.

The Silver Owl Network is on a mission to STOP these fraudsters and protect everyone from getting caught out.

This guide has been designed to help you:

1. **Recognise** when an email could be a potential threat.

2. **Know** what action to take, if you think you have got a scam email.

3. **Understand** how you can protect against scam emails in the future.

The Silver Owl Network

Key Words

Email '**SCAM**' – General term used for any email which is sent with the intention of 'swindling' the person receiving it. This includes any attempt to steal your money, waste your time or cause you distress.

Email '**FRAUD**' – The formal action of sending emails intended to defraud.

Email '**SCAMMERS**' – Word used to describe the person(s) sending these emails.

'HACKERS' – General term for anyone using technology to try and access your private information or banking details.

'VIRUS' or **'TROJAN'** – Types of software that, when downloaded onto your computer or laptop, cause your computer to stop working, work incorrectly or unwittingly share the information on your computer with other people.

'PHISHING' Emails – Emails that are sent out randomly hoping to catch people out (from the normal phrase 'to fish').

Want to know the meaning behind other 'modern technology' phrases?

Visit us at www.SilverOwlNetwork.co.uk for more information.

The Silver Owl Network

What are the top 3 types of email scam?

An email scam is where someone pretends to be a person or organisation you trust in order to get money or information out of you.

There are 3 types of email scam:

1. ***Someone pretends to be a person you already know***

These emails will appear in your inbox with the 'from' email address column being one you recognise from your immediate address book. Say if you have a good friend Barbara Smith who uses email b.smith@btinternet.com then this would appear to be the 'from' sender.
The content of the email will be urgently requesting help. Some of these types of email will state that your friend is on holiday somewhere and has had all their cash stolen so they need you to send them some money.
The important thing to remember here is that scammers will want to frighten you, they will want to make their email seem very important and urgent to deal with.

2. ***Someone pretends to be an organisation you <u>USE</u> and <u>TRUST</u>***

The purpose of each email is to get you to part with your money so these are usually from organisations that everyone would use. High street banks, HMRC office etc.. The email might look exactly like others you have received. Hackers can get access to all the colours, logos and templates of the actually companies so can make their emails look identical to the genuine ones.

3. ***Someone pretends to be an organisation you <u>DON'T USE</u> but <u>DO TRUST</u>***

These emails will not be from a bank or tax office but more likely a paid service like a delivery courier. A good example is an email that appears to be from Parcelforce (the popular delivery courier) and it is requesting that there is a parcel being held for you but the postage needs paying before it can be released.

The Silver Owl Network

Simple Ways To Deal with Email Scams

Make sure that you know how to deal with these potential scam emails while not ignoring any genuine requests for information.

Step 1:

Always call the person or company from which the email appears to have come from.

NEVER use any of the contact details within the email to do this, only use telephone numbers you already know (or can find on their company paperwork).

Step 2:

Don't worry if it is 'out of hours' or over the weekend.

Scammers who send these emails want you to think that responding to their email is your only option. It isn't. No company would take any action against you outside of their normal working hours.

Step 3:

Don't worry about asking for help. Scam emails are very common and are made to fool you. We deal with hundreds of potential emails and know how best to help you.

3 Ways you can stop future scam emails

Step 1:

Set up a second email address and use this to channel all of your non important contact through. So, if a website wants you to sign up to a newsletter before it will let you see a news item, use your second email address so you don't get these useless messages caught up in your proper email account.

Find out how to set up a second email by visiting our website at **www.SilverOwlNetwork.co.uk** and go to the 'support' page.

Step 2:

Keep a written list near your computer (or laptop) of all the telephone numbers of people or companies that are important or relevant to you like:

- The mobile numbers of friends or family
- Your bank contact telephone number
- Your accountant/Solicitors telephone number

Step 3:

Become familiar with the ways to detect a scam email. For example, find out how to view the email address of the sender of the email. A lot of common business scams pretend to come from the name of the person you know but the email address is not the same.

Example:

Email says it is 'from' Margaret Smith' but the actual email address is NOT the one you know, ie m.smith@dodgey.email.server.com

Also, try and include any email addresses you have for them or their fraud departments, this way you can send them a separate email (NEVER respond to the email you have received **OR** send it on to anyone else in case it has a virus in it).

Also, look out for bad spelling or incorrect grammar. Sometimes it can be as simple as a few words misspelt for you to get a hint that it is not genuine.

Would your bank or accountant send an email with lots of spelling mistakes? Probably not.

Ask yourself, would my bank demand an instant answer to this question? Would HMRC or the government demand attention without sending me a letter in the post?

Summary

It is the job of email scammers to come up with new ways to deceive us. If you follow these simple rules, you can stay safe and feel confident about what to do if you should receive an email you think could be a scam.

Don't worry. No genuine company or person would take immediate action against you.

Make contact. Call the person or company, if possible, to check whether the email is valid. NEVER use the contact details inside the email.

Join our Silver Owl Network. You can join us for free and gain access to all our free guides and information.

We won't be happy until EVERYONE is safe online.

Think you might have received a SCAM EMAIL. You can call us using our FREEPHONE telephone number on 0800 043 8700 or email info@SilverOwlNetwork.co.uk