Dealing with Spam Emails & Calls

Mendlesham Computer Club

By Giles Godart-Brown

What are we dealing with?

Spam = unwanted messages, adverts and calls.

Scam = an attempt to trick you into losing money, information or access.

Phishing = messages designed to make you click, sign in, pay or reveal information.

Scammers can contact you by email, phone, text, social media or messaging apps.

The same rule works everywhere: STOP before you act.

The biggest warning signs

- URGENCY — “Act now”, “within 24 hours”, “your account will be closed”.
- AUTHORITY — pretending to be your bank, HMRC, police, delivery company or a relative.
- EMOTION — fear, panic, excitement, guilt or a tempting prize.
- MONEY or INFORMATION — asking for passwords, PINs, codes, bank details or payment.
- UNEXPECTED — you were not expecting the contact.

Spam email: what to look for

- Look at the sender — does the address really belong to the organisation?
- Be suspicious of unexpected invoices, refunds, parcels, account warnings and password resets.
- Hover over links (without clicking) to see where they really go.
- Unexpected attachments can contain malware.
- Poor spelling is no longer a reliable test — modern scams can look very professional.
- QR codes in emails can also lead to scam websites.

The safest way to check an email

- DO NOT use the link, phone number or email address supplied in the message.
- Open your browser or use an app you already know is genuine.
- Find the organisation's official website yourself.
- Use the phone number on your bank card, statement or official website.
- If you are still unsure, ask someone you trust before doing anything.

Never let the message choose how you verify it.

How to reduce unwanted emails

- Use your email provider's “Spam” or “Junk” button.
- For a genuine company you recognise, use its unsubscribe link.
- If the sender is suspicious, DON'T click “unsubscribe” - mark it as spam instead.
- Keep your main email address private where practical.
- Consider a second email address for newsletters, shopping and competitions.

How to stop emails going to Spam or Junk folders

- Check the Spam/Junk folder regularly — especially if you are expecting an important email.
- If you know the sender is genuine, select the message and choose “Not spam”, “Not junk” or similar.
- Add the sender’s email address to your Contacts or Address Book.
- If your email service has a “Safe Senders” or “Trusted Senders” list, add the sender there.
- For a trusted newsletter or mailing list, add the sender or domain rather than switching off spam protection.

Don’t switch off spam protection — teach it which senders you trust.

Gmail and Outlook — the simple approach

- GMAIL: Open Spam → select the genuine message → "Not spam". Adding the sender to Google Contacts can help future messages reach your inbox.
- OUTLOOK: Open Junk Email → select the genuine message → "Not junk". You can also add the sender or domain to Safe Senders.
- IMPORTANT: Only do this when you are confident the sender is genuine.
- If a message still goes to Spam after these steps, the sender may have a delivery problem that only the sender can fix.
- Never add a suspicious sender to your Safe Senders list just because you want to see what they are sending.

SAFE SENDER = someone you have independently checked.

“Hide My Email” — keep your real address private

- Instead of giving a website your real email address, use a special, random email address (an alias or “mask”).
- Messages sent to the alias are forwarded to your real inbox - the website does not see your real address.
- This can reduce unwanted mail and makes it easier to stop messages from one website: disable or delete that alias.
  - You can set this up by getting another gmail account and setting it to forward all mail to your real inbox.
  - Apple’s “Hide My Email” is available with iCloud+. On an iPhone, Safari can offer it when a website asks for your email address.
  - Other services, such as Firefox Relay, also provide email masks.

Spam calls

Mendlesham Computer Club

By Giles Godart-Brown

Spam calls: you are allowed to hang up

- If an unexpected caller makes you uncomfortable: HANG UP.
- Do not confirm your name, address, date of birth, bank details, PIN or passwords.
- Do not install software or give someone remote access to your computer.
- Do not press buttons to “speak to an adviser” if you suspect a scam.
- Do not call back an unfamiliar number just because it rang once.

A very useful phrase

“I never make financial decisions on an unexpected call.”

Then hang up.

- Wait a few minutes if you feel pressured.
- Call the organisation back using a trusted number you found yourself.
- Remember: genuine organisations will understand you checking.

How to reduce nuisance calls

- Consider registering your landline/mobile number with the Telephone Preference Service (TPS).
- Use your phone's spam-call screening and blocking features.
- Block repeat nuisance numbers.
- Don't rely on caller ID alone - scammers can make calls appear to come from genuine numbers.
- Tell friends and family what sort of calls you want them to help you check.

7726 — remember this number

7726 = SPAM

- Most UK mobile networks let you forward suspicious texts to 7726 for free.
- You can also report a suspicious scam call to 7726.
- Your mobile provider can investigate and potentially block the sender.
- Do not reply to a suspicious message just to say STOP.

What to do next

Mendlesham Computer Club

By Giles Godart-Brown

What if you clicked the link?

- Don't panic. A click does not automatically mean you've been hacked.
- If you entered a password, change it immediately -
  and change it anywhere else you reused it.
- If you entered bank/card details, contact your bank immediately.
- If you installed software at the scammer's request, run a full antivirus scan and get help.
- Never install software that allows someone else to take over your PC
  e.g. Teamviewer
- Watch your accounts for unusual activity.

What if you've lost money?

CONTACT YOUR BANK IMMEDIATELY

- Use the number on the back of your card, your bank's official app/ website, or another trusted contact method.
- If your bank supports it, 159 can connect you safely to your bank.
- Report fraud: England, Wales & Northern Ireland — Report Fraud.
- Don't be embarrassed. Scammers are professionals; acting quickly matters.

A simple 10-second routine

1 STOP	2 CHECK	3 ACT	4 REPORT

1. STOP — don't click, reply, pay or give information.
2. CHECK — contact the organisation independently.
3. ACT — only when you are satisfied it is genuine.
4. REPORT — so others may be protected too.

Quick quiz: what would you do?

1. Your “bank” calls and says you must move money to a safe account. → ?
2. An email says your parcel is waiting and asks you to pay £2.99. → ?
3. A company you recognise emails a newsletter you no longer want. → ?
4. A text from an unknown number says “Are you free to talk?” → ?
5. You clicked a suspicious link but entered nothing. → ?

STOP · CHECK · REPORT

Answers

1. Hang up. Call your bank using a trusted number.
   Never move money because an unexpected caller tells you to.
2. Don't click. Check the delivery company independently.
   Be wary of unexpected payment requests.
3. Use the genuine unsubscribe link if you recognise the sender.
4. Don't reply if the sender is unknown. Report suspicious texts to 7726.
5. Don't panic. If no information was entered or software installed,
   stay alert and monitor your accounts.

Three things to remember

1 Don't be rushed

2 Verify independently

3 Ask for help if unsure

It is OK to say: “I need time to think about this.”