# Spotting Phishing and Social Engineering

Phishing is an attack in which a criminal sends a message that pretends to come from someone we trust, hoping that we will click a link, open a file or hand over private information. It is one kind of social engineering, which means attacking people's habits and emotions instead of breaking into computers. Salma, an accounts payable officer at a manufacturing company, uses five habits every day to stay ahead of such messages, which can arrive by email, text message, chat or phone call. This video is a teaching aid, so the security team's own rules should always be checked.

## 1. Know the Trick

Social engineering works because it uses normal human reactions, such as respect for authority, urgency and strong emotion. Attackers use information found online, including on social media, so a message can mention real names, projects and suppliers and still be a trap. Polished writing is no longer proof of honesty, because tools can now produce flawless text. The first habit is to ask what action the message really wants, whether it is a click, a payment, a password or an opened file.

**Example:** A new employee at a law firm receives a chat message that uses the managing partner's name and photo and asks for gift cards for a client. The employee asks what action the message wants and sees that it is a purchase made through chat. Instead of buying, the employee checks with the office manager, and the request stops there.

**At work:** Salma receives an email that greets her by name, mentions a real supplier and refers to a genuine purchase order. She remembers that such details can be collected from public pages, so they prove nothing. She asks what the email really wants, and the answer is a change of bank account. She does not reply, and she checks the request first.

## 2. Slow Down

Pressure is the attacker's best tool, because a person in a hurry skips the checks. Typical messages say that an account will be closed, a payment is overdue or a senior executive needs something before a meeting. Official advice lists urgent, emotional language and threats of serious consequences among the signs of phishing. The second habit is to pause when we feel rushed and to treat the feeling itself as a warning.

**Example:** A text message says that a parcel will be returned unless the recipient pays a small fee within one hour. The recipient feels the rush, pauses, and notices that no order number appears anywhere in the message. Tracking the parcel on the courier's own website shows nothing waiting, so nothing is paid. That is exactly what slowing down means.

**At work:** An email that seems to come from Salma's finance director asks for an urgent transfer to a new supplier before noon. She notices her own sense of panic and treats it as the signal to slow down. She calls the director on the number in the company directory. The director knows nothing about the request.

## 3. Inspect the Sender and Links

The third habit is to look closely at where a message really comes from and where it leads. The display name can say anything, so we check the full address for a swapped letter, an extra word or an unusual domain. A link can show one name and lead to another, and hovering the pointer over it shows the real destination without a click. We do not trust shortened links, which hide the destination, and we are careful with unexpected attachments.

**Example:** A message that claims to come from a bank uses an address with two letters swapped in the bank's name. The two letters look alike at a glance, which is exactly why the trick works. The customer inspects the full address, deletes the message and opens the bank's own app. That is what inspecting the sender means in practice.



This document is a property of Asaseeyat Academy - © Copy Right Protected.

**At work:** Salma receives a link to a supplier's invoice portal, and the sender's name looks perfectly normal. Hovering over it shows a website unrelated to the supplier, so she does not click. She phones the supplier's accounts office on the number in the contract. She learns that the supplier's mailbox was taken over that morning.

## 4. Verify Unusual Requests

The fourth habit concerns what the message asks for. Requests for passwords, payments, gift cards or a change of bank details need a second check, whatever name is on the message. We confirm the request through a channel we already know, such as the number in the contract, and never through contact details inside the message. Banks do not ask us to confirm account details over the phone, so a caller who does is a warning sign.

**Example:** A caller who claims to be from the bank asks for the code that was just sent by text message, saying it will protect the account. The account holder hangs up and calls the number printed on the bank card. The bank confirms that it never called, so the account stays safe. That is why unusual requests are always verified.

**At work:** A supplier's email tells Salma that its bank details have changed and asks her to use the new account from the next invoice. She follows the company rule that every change is confirmed by a call to the number in the contract. The supplier says nothing has changed, so her call stops a payment that would have gone to a criminal.

## 5. Report Quickly

If a message looks suspicious, we do not reply, click, open an attachment or call a number inside it. We report it through the organisation's own channel, such as a report button or the security team, and many email services also offer a report spam option. Reports matter because they show the security team which attacks are in use. If someone has already clicked or shared information, the security team is told at once and the exposed passwords are changed. Reporting is never a reason for blame, because anyone can be tricked, and people who fear punishment may stop reporting.

**Example:** A message that looks like a prize notice reaches a personal phone, promising a free holiday if the owner taps a link. The owner does not reply or click. The owner uses the phone's report spam option and deletes the message, and the report reaches the service. That is exactly what reporting quickly means.

**At work:** Salma doubts an email that says the company mailbox is almost full and asks her to sign in through a link. She does not click, and she uses the report button instead. The security team checks the message and warns the colleagues who received the same one. One report protects many colleagues.

## Conclusion

In summary, phishing and social engineering try to make people act fast and carelessly. Five habits help us resist them: knowing the trick, slowing down, inspecting the sender and links, verifying unusual requests and reporting quickly. When in doubt, we stop and verify through a channel we already trust. Salma's calm routine shows that each check is quick and that stopping to verify is worth the time. This video is a teaching aid, so the rules of the organisation's own security team come first.

### Sources


- CISA (US Cybersecurity and Infrastructure Security Agency): Recognize and Report Phishing (signs of phishing, report spam, verify independently) – https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
- CISA: Avoiding Social Engineering and Phishing Attacks (definitions, hovering over links, verifying through known contacts, what to do if compromised) – https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
- UK National Cyber Security Centre (NCSC): Phishing attacks and scams (public information used by criminals, why reporting helps) – https://www.ncsc.gov.uk/collection/phishing-scams
- UK NCSC: Spot scam messages, emails, calls and texts (authority, urgency, emotion; banks do not ask to confirm account details by phone; contact the organisation directly) – https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams
- UK NCSC: Phishing attacks, dealing with suspicious emails (no blame culture, reports show which attacks are in use) – https://www.ncsc.gov.uk/guidance/phishing
- All five pages were opened on 26 Oct 2026 with the fetch tool (page text read).




This document is a property of Asaseeyat Academy - © Copy Right Protected.