ME/PSO

HANDBOOK

# Email Security Handbook

Protection against phishing, malicious attachments and email fraud

*Companion material for the training course:*
***“Email Security”***

Document No. MEPSO-PRI-MAIL-002 · Classification: Internal Use
Information and Cyber Security Department · MEPSO AD Skopje

# Contents

# 1. Introduction

Email is the most widely used business communication tool — and precisely for that reason, the most common entry point for cyber attacks. Over 90% of successful attacks begin with an email.

This handbook will help you recognize the threats that arrive by email and develop habits that protect you and the organization. It will not make you a technical expert — it will make you an attentive and informed user, which is more important.

Every day you receive dozens of messages. Among them, occasionally, hides one designed to deceive you, steal data or install malware. The difference between a secure and a compromised system is often a single click.

> **Key thought.** The most sophisticated security systems can be bypassed with one well-crafted email that tricks a person into clicking. You are the most important protection.

# 2. Why email is a target for attacks

Attackers love email for several reasons:

- **Reach** — a single message can be sent to thousands of people at once;
- **Trust** — people are used to opening messages and clicking links;
- **Easy impersonation** — it is relatively easy to pretend to be someone else;
- **Direct access** — email leads straight to the user, bypassing many technical protections;
- **The human factor** — exploiting curiosity, fear or urgency.

## 2.1 What they want to achieve

| Goal | Method |
|---|---|
| Stealing passwords | Fake login pages |
| Installing malware | Infected attachments |
| Financial fraud | Fake invoices, transfer requests |
| Data theft | Manipulating you into disclosing information |
| Access to systems | Compromising a user account |

# 3. Anatomy of an email threat

To recognize a suspicious message, it is important to know the elements attackers exploit.

### 3.1 The sender's address

The most important element to check. Attackers use addresses that resemble legitimate ones, with small differences that are easy to miss — a swapped letter, an extra character, a similar domain.

> **Watch out.** An address like mepso-it.com is not the same as mepso.com.mk. Always check the entire domain, not just the display name.

### 3.2 The subject line

Subject lines are designed to provoke an urgent reaction: “Urgent”, “Your account has been blocked”, “Final warning”. Urgency is a tactic to stop you from thinking clearly.

### 3.3 The message body

Pay attention to generic greetings (“Dear user” instead of your name), grammatical errors, an unusual tone, and requests to do something quickly.

### 3.4 Links and attachments

This is where the real danger hides. Links lead to fake pages, and attachments contain malicious code.

## 4. Phishing — recognition and protection

Phishing is the most common type of email attack. The attacker pretends to be a trusted institution in order to lead you to disclose sensitive data.

### 4.1 Types of phishing

| Type | Description |
|---|---|
| Mass phishing | The same message sent to thousands of recipients |
| Spear phishing | Targeted at a specific person, using personal details |
| Whaling | Targeted at executives and senior positions |
| Clone phishing | A copy of a legitimate message with altered links |

### 4.2 Red flags

- ✓ Urgency and pressure to act quickly
- ✓ A request for a password, PIN or personal data
- ✓ A generic greeting instead of your name
- ✓ Grammar and spelling mistakes
- ✓ A suspicious sender address
- ✓ An offer too good to be true (prizes, winnings)
- ✓ Links that do not match the displayed text

***A phishing example:***
*“Dear user, we have detected unusual activity on your account. To verify it, click here and enter your details within 2 hours, otherwise your account will be permanently blocked.”*
*Signs: generic greeting, urgency, request for data, pressure.*

### 4.3 How to protect yourself

- ✓ Stop before reacting to urgent requests
- ✓ Check the sender's address carefully
- ✓ Hover over the link to see its real destination
- ✓ Type addresses into the browser manually instead of following links
- ✓ Never enter a password on a page you reached through a link
- ✓ When in doubt, confirm via an official phone number

## 5. Malicious attachments

Attachments are a common way of spreading malware. Opening an infected attachment can install a virus, ransomware or spyware.

### 5.1 Dangerous file types

| Type | Risk |
|---|---|
| .exe, .scr, .bat | Executable programs — high risk |
| .zip, .rar | Compressed files that hide their contents |
| .docm, .xlsm | Documents with macros that execute code |
| .js, .vbs | Scripts that execute commands |

**Rule.** Do not open attachments from unknown senders. Even from known ones — if you were not expecting the file, confirm through another channel before opening.

### 5.2 Macros in documents

When you open a document that asks you to “Enable macros” — stop. Legitimate documents rarely require this. Enabling macros can execute malicious code.

## 6. Dangerous links

Links are disguised to look safe, but lead to dangerous pages.

### 6.1 How to check a link

- ✓ Hover over the link (without clicking) — the real address appears at the bottom

- ✓ Check whether the domain matches the one you expect
- ✓ Be careful with shortened links that hide the true destination
- ✓ If the link asks you to enter data, be especially cautious

> **Tip.** If you receive a message from a bank or institution containing a link, do not click it. Instead, open a new window and type the official address manually. That way you can be sure you are on the genuine page.

## 7. Spam and unwanted mail

Spam is unsolicited bulk mail. Although often merely annoying, it can also carry threats.

- ✓ Do not reply to spam — it confirms that your address is active
- ✓ Do not click “unsubscribe” in suspicious messages — it may be a trap
- ✓ Mark spam to improve filtering
- ✓ Do not publish your business address in public places unnecessarily

## 8. Business email compromise (BEC)

Business Email Compromise is a sophisticated attack in which the attacker pretends to be an executive or a partner in order to induce a financial transaction or the disclosure of data.

### 8.1 A typical scenario

You receive a message that appears to come from a director, urgently requesting a transfer of funds or the sending of confidential data. The tone is authoritative and urgent.

> **Warning.** Any unusual request for a transfer of money or confidential data, even if it appears to come from a manager, must be confirmed through a direct phone call or in-person communication.

### 8.2 Protection

- ✓ Verify unusual financial requests through a second channel
- ✓ Watch out for changes in payment details
- ✓ Do not rely on email alone for important transactions
- ✓ Report suspicious requests immediately

## 9. Encryption and privacy

Sensitive information sent by email must be protected.

- ✓ Do not send passwords or confidential data in plain text
- ✓ Use encryption for sensitive attachments where available

- ✓ Pay attention to whom you are sending — double-check the recipients
- ✓ Avoid “Reply all” unless it is genuinely necessary

**A common mistake.** Accidentally sending confidential information to the wrong recipient is a frequent incident. Always check the recipient's address before pressing “Send”, especially when autocomplete suggests an address.

## 10. Good everyday habits

- ✓ Review messages carefully before reacting
- ✓ Check the senders' addresses
- ✓ Do not click links or attachments at the slightest doubt
- ✓ Use a strong and unique password for your email
- ✓ Enable two-factor authentication
- ✓ Log out of your email on shared devices
- ✓ Report suspicious messages

## 11. What to do in an incident

If you have clicked a suspicious link, opened an attachment or entered data somewhere you should not have:

1. Do not panic — a quick reaction is key
2. Disconnect from the internet if you suspect malware
3. Immediately change the passwords you entered
4. Report to the Information Security Department
5. Do not delete the message — it may serve the analysis

**Do not be ashamed to report.** Anyone can make a mistake. Prompt reporting allows the security team to react and limit the damage. Silence only makes the problem worse.

## 12. Practical scenarios

### Scenario 1: An urgent message from “the director”

You receive an email supposedly from the general director, urgently asking you to pay an invoice to a new account, “because he is in a meeting and cannot take calls”.

**Correct reaction:** You do not act immediately. You confirm directly with the director or through an official channel. Urgency and the impossibility of verification are classic signs of BEC fraud.

**Scenario 2: A forwarded invoice**

A colleague forwards you an invoice for payment with an attachment. The attachment asks you to enable macros in order to view the contents.

**Correct reaction:** You do not enable macros. You check with the colleague whether they really sent it and whether macros were expected. Legitimate invoices do not require macros.

**Scenario 3: A parcel notification**

You receive a message saying you have an undelivered parcel and need to click a link to pay for the delivery.

**Correct reaction:** You do not click. If you are expecting a parcel, you go directly to the courier service's official website. Fake parcel notifications are very common.

## 13. Frequently asked questions

### How can I tell whether a sender's address is fake?

Check the entire domain carefully, not just the display name. Look for small differences — swapped letters, extra characters, a similar but not identical domain.

### Is it safe to open a PDF attachment?

PDFs are generally safer than executable files, but they too can contain malicious code. Open them only from trusted senders whose files you were expecting.

### What if I clicked a link but did not enter anything?

Report it anyway. Some links can install malware merely by being opened. The security team will assess whether there is a risk.

### Does the spam filter protect me completely?

No. Filters catch a lot, but not everything. The most sophisticated attacks often get through. Your vigilance remains essential.

### Can my password be stolen just by opening a message?

Rarely, but it is possible with some advanced attacks. That is why you should not open messages from unknown senders, and never enter data through a link from a message.

## 14. Glossary and checklist

| Term | Meaning |
|---|---|
| Phishing | Fraud via fake messages aimed at stealing data |
| Spear phishing | Targeted phishing aimed at a specific person |
| BEC | Business email compromise — fraud through a fake identity |
| Malicious attachment | A file containing harmful code |
| Macro | An automated command in a document; can be abused |
| Spam | Unsolicited bulk mail |
| Domain | The part of the address after the @ sign |

### A quick checklist before every click

- ✓ Do I know and expect the sender's address?
- ✓ Does the subject create artificial urgency?
- ✓ Does the message ask for a password or personal data?
- ✓ Where does the link really lead (checked by hovering)?
- ✓ Was I expecting this attachment?
- ✓ When in doubt — did I report instead of clicking?

## The role of email in MEPSO's operations

As an operator of critical infrastructure, MEPSO carries a heightened responsibility for protecting its communications. Email often contains sensitive operational and business information whose compromise could have consequences beyond the organization itself.

### Additional measures for critical infrastructure

- ✓ Operational data is never sent over unprotected channels
- ✓ Communication with external partners is subject to additional verification
- ✓ Access to business email from personal devices is controlled
- ✓ Phishing simulations are conducted regularly to raise awareness

> **Shared responsibility.** Email security is not just the IT Department's job. Every employee who handles email is part of the organization's defense system. Your habits directly affect the security of the entire infrastructure.

### Periodic training

Threats constantly change and grow more complex. That is why it is important to refresh your knowledge regularly through training and stay informed about new fraud methods. This handbook is part of that continuous education.

## 15. Conclusion

Email will remain a central part of work — and a central target of attacks. Your vigilance is the best protection. Every message you check carefully, every suspicious link you do not click, every report you make — all of it builds MEPSO's security.

> **Remember.** When in doubt, stop and ask. One minute of caution can prevent a major incident.

---

MEPSO AD Skopje — Electricity Transmission System Operator of North Macedonia
Document No. MEPSO-PRI-MAIL-002 · Classification: Internal Use