Tip sheet

BEST PRACTICES FOR EMAIL HYGIENE

Just like a physical letterbox, electronic mailboxes accumulate official correspondence, order and delivery tracking, advertisements, scams, and many other items. Managing your electronic mail (email) is therefore just as important as managing your paper mail. However, email is accessible online and can be open to exploits, making the securing of exchanges and personal data protection a challenge. Best practices, known as email hygiene, should therefore be adopted, both for the mailbox receiving electronic mail and for the email address itself.

Protecting and securing your professional email address

Your institution or establishment has assigned you an email address. As such, you represent both it and yourself. Responsible use is therefore essential to, in particular, lend credibility to your communications and maintain a good image of yourself and your employer, but also to protect your privacy and the security of the institution or establishment you belong to.

Do's

Choose a strong and unique password

The password for your professional email account must be complex (mixing letters, numbers and symbols), unique and changed on a regular basis.

enhanced information security, reduced risk of hacking

Tip!

If the option is offered and available on your email inbox, activate two-factor authentication (2FA) for an extra layer of security.

Report any suspicious emails

If an email seems suspicious or fraudulent to you, report it to your IT department, or to Restena Foundation's CSIRT service (csirt@restena.lu). Report it at the slightest doubt, even if it seems pointless to you. Only those responsible for security can judge the relevance of the information.

Also, if you receive an email from a known institution/company/bank and you are not sure of its legitimacy, check with this institution through other means of communication (by telephone for example) or by visiting its official website.

improvement of anti-spam and anti-phishing security filters

Did you know?

Reporting suspicious emails is a responsible approach that helps not only protect your own online security but also preserve that of the entire research and education community.

Don'ts

Store your password in 'plain text'

Don't write down your passwords in plain text on a notepad or post-it note, and do not save them in a text document or spreadsheet on your computer or smartphone.

account and/or privacy breach

Tip!

Manage your passwords with a password manager. The open-source identification platform Passbolt, for example, is developed in Luxembourg.

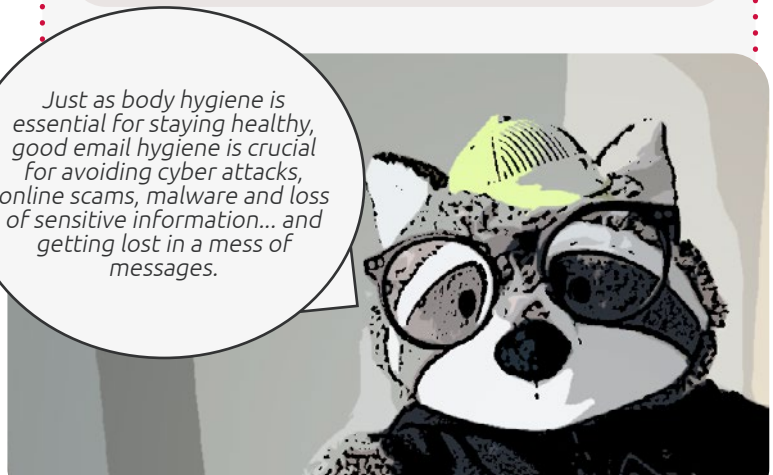
Open suspicious attachments and links

Be wary of emails from unknown or unusual sources. Is the sender unknown to you, is the email subject alarming, and/or are you receiving an unexpected attachment? Don't click on unsolicited links and don't open attachments.

phishing attempt, virus

Tip!

Do you have doubts about an email? Report it as suspicious and then delete it immediately.



Respect the confidentiality of transmitted information

Before sharing any confidential or sensitive information, ensure that additional security measures, such as encryption (PGP/GPG, S/MIME), are implemented on your email account. In order to do so, turn to your IT department.

Otherwise, or if you don't know the level of security of your email account, prefer using secure sharing tools.

data confidentiality, secure communications, integrity of exchanged information

Did you know?

FileSender, Restena's large file sharing service, has a "zero-knowledge encryption" option.

Secure remote connections

For optimal security of electronic exchanges, the TLS cryptographic protocol must be activated on both servers and the email client. Although email server security is the responsibility of the service provider, you can manually activate TLS in your client programme for both incoming and outgoing emails.

protection of sensitive data, minimisation of cyber-attack risks

Use your address for private or personal purposes

Your professional email address should be reserved for communications related to your professional activity. Consult and follow your establishment's policy regarding its use. Authorised use of confidential information and online practices are generally listed and shared in an IT charter.

In any case, don't use it to register for non-professional services (social networks, private portals) or on public/private forums or platforms.

data breach/violation, address compromise, spam, phishing attempt

Tip!

Make a clear distinction between your professional and private addresses.

The **TLS protocol** (Transport Layer Security) encrypts the exchange of connection information (access code) and the receipt and sending of emails between an email client (mailbox) and email servers.

With the TLS, exchanges sent by and received on your email address are protected.

Two-factor authentication is an authentication method requiring two distinct proofs of identity.

In addition to the password, there is an additional authentication factor: unique code sent by email or SMS, authentication application, physical key or biometric data.

Encryption converts data from a readable format to an encoded format. The data can only be read by the person(s) holding the correct encryption key.

Encrypted data intercepted by an unauthorised person is unreadable and unusable. In electronic messaging, the PGP/GPG, S/MIME computer protocols ensure this protection.

Protecting and securing your mailbox

In addition to an email address, your employer provides you with an electronic mailbox. As such, they are responsible for its security. They are particularly responsible for protecting the technical infrastructure where mailboxes are hosted. This first level of security is not sufficient, however; each person individually has a role to play in protecting their own mailbox.

Do's

Organising your mailbox

If you receive a large volume of emails daily, rigorous organisation is essential. Without a clear structure, you risk losing overview of your emails, leading to delays in processing messages or even loss of important emails. Use folders and filters to organise your emails, and file them regularly.

control of your inbox, improved project management and monitoring

Delete unnecessary emails

Irrelevant emails should be deleted regularly. They contain numerous data, potentially sensitive, which could be "stolen" if the mailbox is compromised.

limitation of data leak risks

Archive emails on a regular basis

Regularly archive emails that you wish to keep but which are not appropriate to keep in the inbox.

preserve available space without deleting messages

Keep your user profile up-to-date

The user profile information associated with an email address is crucial. Beyond technical configurations, they are essential in case of loss of access to your mailbox. Such information must therefore be verified and updated regularly.

efficiency and speed of support in case assistance is needed

Did you know?

An article in the General Data Protection Regulation (GDPR) requires that personal data be accurate and, where necessary, kept up-to-date, and that all reasonable steps be taken to delete or rectify inaccurate data immediately.

Dont's

Send large files

To keep your inbox light and avoid size limit problems for sending, sending large attachments by email is not recommended.

overload of available space, impossible to send files exceeding authorised sizes

Tip!

Use large file transfer services, such as (Restena's) FileSender.

Use the mailbox as storage and/or backup space

Your inbox should be dedicated to emails. It is not a place to store or even back up documents or large files long-term.

overload of available space, data leaks in case of breach

Tip!

- Use local backup or cloud backup to store and preserve your important information. However, make sure to consult and respect your institution's policy in this regard.
- If possible and authorised, consider additional protection such as encryption of stored data.

Store sensitive data

Personal, financial or confidential information (passwords, credit card numbers, medical or school records, etc.) should not be kept in a mailbox without appropriate protection such as PGP/GPG, S/MIME.

data leaks in case of breach

Tip!

Move/archive any email containing sensitive data out of your mailbox if it is not encrypted using PGP or S/MIME protocols.

Is your professional messaging service managed by Restena?

- Check and keep your user profile information up to date, such as your identification data (postal address, etc.) by connecting to the "Online Account Management" tool at account.restena.lu
- The use of TLS protocol version 1.2 or higher is mandatory for any connection to Restena's email servers. The email clients you use must comply with this security requirement to be able to receive and send emails.

DISCOVER (OR REDISCOVER) IN THE SAME SERIES...

- 'Carefully select a password'
- 'Spam & phishing messages'
- 'From a cyberattack to data acquisition'
- 'Social engineering attacks'
- 'Back up your data safely'

LU ET APPROUVÉ PAR HEX

Service offer

The Restena Foundation offers a secure, high-performance, and high-availability email hosting service and manages the Professional email messaging for teachers in Luxembourg.

For more information on those services, please visit restena.lu/en/service/e-mail-hosting and restena.lu/en/service/educationlu-e-mail-messaging-system

Co-funded by the European Union

This tip sheet is one of the awareness-raising activities set up as part of the European LuCySe4RE project that has received funding from the European Union's Digital Europe programme (DIGITAL) under grant agreement No. 101127864.

restena
réseau · sécurité · .lu