SPECIAL ATTENTION

Note that it does not conform to the Medical University of Graz Data Protection and Information Security Policy if:

- You disclose your password.
- You use a password that is weak (too short, a simple word, name, which contains no special characters, no numbers or upper/lower case).
- You use the same password for multiple websites or services.

Be especially attentive if:

- You are prompted to forward data from your email account (including the password) via email or via web form.
- The password is stored with another email provider (e.g. GMX) (Collective Mailbox).
- You use a public Wi-Fi network or have configured Wi-Fi with a password stored on a mobile device.
- An error was reported during a retrieval process of the mails (either in the WLAN of the Medical University of Graz or in other WLANs), and then it resumes service.
- You use eduroam WLAN on an Android device or it has been configured on a mobile device with a stored password.
- Many of your emails are unable to be delivered (bounced). This may be a sign that your address has been abused, or even your account has been taken over!
- Someone attempts to blackmail you or request names, such as those of a supervisor for favours (financial or otherwise).
- **You access the Citrix service from outside the Medical University of Graz.**

HELP WITH QUESTIONS AND PROBLEMS

Contact to our IT-Serviceline:

- Mo - Fr: 6:30 - 17:00 Uhr
- tel: +43 316 385-74444
- mail: it-serviceline@medunigraz.at

Useful Links:

- **Directives and Regulations of the Medical University of Graz:**
  Check out: https://muniverse.medunigraz.at/
  Search key word: IT Regulations

- **Security at your IT-workplace:**
  Check out: https://muniverse.medunigraz.at/
  Search key word: IT-Sicherheit am Arbeitsplatz

Organizational Unit for Information Technology and Digitization
Medical University of Graz
Auenbruggerplatz 2/ 8036 Graz
www.medunigraz.at/it-services/

Medical University of Graz

SPAM - PHISHING ACCOUNT- ABUSE

IT SECURITY GUIDE 2020

WWW.MEDUNIGRAZ.AT

IT SECURITY

Security in IT

IT security is an important issue not only for servers but also for your devices.

Your Organizational Unit for IT is your contact for IT security issues including those related to firewalls, network security for servers, application security at workstations and various threat scenarios including spam, phishing and malware (viruses).

Prevention is the best way to increase security, we can help you take preventive action against hacking attacks, virus contamination, phishing and so on.

Our recommendations and regarding to the use of suitable tools are also published on our website.

SPAM

- The term spam refers to unwanted, mass- sent email messages, in discussion forums or chat systems.
- Where can I get support?
  Please call our **IT-Serviceline with the extension 74444** or send an email directly to: it-serviceline@medunigraz.at.

If in doubt, be sure to ask!

it-serviceline@medunigraz.at

PHISHING

- Emails which include any of the following examples should be examined for validity:
  - „urgent“
  - „last chance“
  - concerning account deletion
  - ask for credentials, credit card numbers, bank account details and bank information for „verification”.
  - request that you check invoices or track packages.
- Common to all is the question of sensitive information and data.
- These emails may lead to misuse or theft of mail accounts, other accounts of the Medical University of Graz, bank accounts and credit card accounts, etc., and may lead to data breaches; if this happens please send a message to the Datenschutzbehörde (data protection officers)!

Your Organizational Unit for IT and the Medical University of Graz follow standard security practices and will never send you a password (especially not in plain text). You should never share your passwords!

- **Always check:**
  1. the sender (what is the real address behind the displayed name?),
  2. The URL that the link will actually open,
  3. the content (spelling, grammar and logic)

More:
https://muniverse.medunigraz.at/Seiten/Phishing-Mails.aspx

Think I am at risk what should I do?

Immediately change your password for the account that was compromised as well as for other personal and company accounts where the same password was used!
Make sure to use unique passwords for every service.

muniverse.medunigraz.at/Seiten/Passwort-Richtlinien.aspx

NEXT STEPS

1. Report the incident to:
   it-serviceline@medunigraz.at with an original, full copy of the phishing email attached (drag & drop).
   If you have any further questions, please contact us at **datenschutz@medunigraz.at**. Do not send the phishing message here - unless absolutely necessary - if necessarily pack in a file archive (e.g., ZIP).

2. If this is a data protection incident it must be brought to the attention of the data protection officers as soon as possible. The best way is to email **datenschutz@medunigraz.at**, and include which systems are affected.

3. **Inform your IT- partner**, so that it can be determined whether a trojan or other viruses have infected your computer/tablet/ phone as well.

TIP:
NEVER go to login pages via a link in an email, instead go directly to the page such as from your favourites or bookmarks!