User Accounts and Password usage

Charles University Realm

 For Charles University Central Autentication Services (**CAS**) please go to https://ldapuser.cuni.cz/

The CERGE-EI realm:

Every faculty and staff member as well as every student are eligible for network and email accounts. These accounts are setup by the network administrator after filling up a simple form by a new LAN user directly at the computer office on the 4th floor, room 409. **CERGE-EI email accounts are "lifetime" accounts for all alumni, provided they are looked after by users. The size of mailboxes can be extended upon request in justified instances by contacting the Computer Office at helpdesk@cerge-ei.cz.**.

The initial password for each account is generated and is unique.

Changing Password (Domain account)

Option A: Via Windows - once you are logged at the PC connected to CERGE-EI internal network:

To change your network password while logged in the LAN using Windows Active Directory, simply press Ctrl-Alt-Delete and then choose the Change Password option.

More details about changing password and its consequences are described in Password Change article.

Option B (experimental): **via Password management Portal (PWM)** available at https://portal.cerge-ei.cz/pwm

PWM is a self-service facility which allows users to:

- Review the user account settings (expiration, password change history, SMS contact, email address)
- **Change** the domain password
- **Reset** forgotten password
- **Register your mobile phone** to be able to reset forgotten password

Important notice:

PWM is in test/experimental phase. Not all users are currently enabled. If you want to use it, please contact IT Office. One of the prerequisities is to have separated your email account from your domain account. It may be achieved by resetting email password via mailserver's web interface. Consult with IT before you start.

–

PLEASE, do not try to change Domain account password via Zimbra webmail, it could lock your network account in some cases.

Sharing identity?

REMEMBER!

Account identified by username is allocated personally to you, you are not allowed to lend it to other people. You are responsible for the activities under this identification.

Password complexity requiremets

Our security settings require that users' passwords meet **complexity requirements** and they are enforced when passwords are changed or created.

Complexity requirements are listed in the Password Change article.

Password usage tips

It's highly recommended to use **strong passwords**, which **does not contain** the user or company name, real name or a complete dictionary word.

Do **NOT** use the **same password** for multiple logins (e.g. the same password for gmail, facebook, windows domain authentification at work, dropbox etc.): when login credentials of one of them is compromised, all the services using the same password should be considered compromised too!

It's difficult to remember a whole bunch of complex passwords, therefore it's recommended to use a password manager, for instance www.lastpass.com for online usage or software based for offline usage http://keepass.info/: you have to remember only one strong “master” password - the others are stored safely in a “vault”.

You can even use the **same strong password** for multiple logins, just add a “service identificator_ckgedit_QUOT_ - example for gmail would be “sTRONgPassW0rd@gmail”, example for facebook could be “sTRONgPassW0rd@FB” - but security is lower than in separate complex passwords..

Make sure you know **how to reset the password** for all of your websites, services, computer accounts you have. In most cases, new password activation link is send to your email filled in during registration. Some services use 2way authentification verification as most banks do, e.g. cell phone SMS.

If you accidentally left behind your smartphone somewhere, **reset immediately** the password for all the services used on the phone - eg. Facebook, email accounts. Attacker could gain access to these services and perform identity theft on you.

Encrypt your entire phone (e.g. Android has already added this feature), encrypt the entire disk of

your laptop using windows Bitlocker or Truecrypt version 7.1a max. - newer versions are not considered safe. In case of theft/loss your data are safe because of encryption.

Passwords should be **changed regularly**. Stronger password could be changed less often, anyway a rules of thumb is: “the period of password change should always be shorter than approx. amount of time needed to crack it.”

Do not tell a password to anyone! If you have to tell a password to somebody else e.g. in order to complete an important task, change it immediately after the usage then.

Do not send passwords by email! Emails travel through internet in plain text form and it is relatively easy to capture an email. Better ways how to share a password are SMS or to tell it during a phone conversation.

Do not react to the **forged emails** telling you to change your password to some of your accounts somewhere. This social technique is called “**Phishing**”.

Do not write passwords on piece of paper, stickers etc.: anybody accessing your table can **abuse them**.

From:
https://wiki.cerge-ei.cz/ - **CERGE-EI Infrastructure Services**

Permanent link:
https://wiki.cerge-ei.cz/doku.php?id=public:user_accounts&rev=1637758852

Last update: **2021-11-24 13:00**