Important information about information security

Current Occasion:
In the **in-house print shop**, **customers' storage media** were contaminated with **malicious code** for an unknown period of time**.** If you have printed there recently, you should avoid connecting the used data media to a computer without up-to-date and active virus protection.

How can you protect yourself and your colleagues?

- Protect mobile data carriers (e.g. USB sticks) and your laptop from unauthorized access, manipulation and loss. They should not be left unattended during business trips. If possible, data should be transported in encrypted form. Do not connect any data carriers to a third-party system to prevent the spread of malware.
  More information at: https://hilfe.uni-paderborn.de/Daten_sicher_aufbewahren/en

- Also carefully examine e-mails from senders that you are familiar with. Is the language correct? Is their request realistic? Before opening links or attachments: When in doubt, you can ask the supposed sender in a new e-mail (not as a reply to the one you received!) whether they have actually sent you anything.
  More information at: https://hilfe.uni-paderborn.de/Hinweise_zu_Phishing-E-Mails/en and https://hilfe.uni-paderborn.de/Signierte_E-Mails/en

- Always keep your operating system, antivirus program and your other programs up to date. Newly released updates should always be installed as soon as possible. Computers with operating systems that are no longer supplied with continuing security updates must be protected from third-party access. If an update is not possible, protection must be guaranteed through alternative measures.

  In addition to Windows Defender, the IMT offers Sophos Antivirus. This service is designed for employees, students and various departments of the University of Paderborn (faculties, institutes, professorships, facilities, committees, university groups) and includes the manual or automatic supply of workstations with up-to-date antivirus software via update servers.
  More information at: https://hilfe.uni-paderborn.de/Antivirensoftware (german) and https://support.home.sophos.com/hc/en-us/articles/360029301731-Sophos-Home-Getting-started-guide

  Windows XP (security update supply was discontinued in April 2014), Windows Vista (security update supply was discontinued in April 2017), and Windows 7 (security update supply was discontinued in January 2020) should no longer be connected to the University's network.

Operating systems such as Mac OS X and Linux must also be kept up to date. This also applies to mobile operating systems such as IOS and Android. Anyone who continues to operate these systems without further security measures is acting with gross negligence.

- Back up your system regularly. A backup makes it much easier to restore your PC to the state you were familiar with and data - even if deleted or encrypted - can be restored. Backups should be stored separately from systems. It is recommended to keep backups in a secure off-site location, without connection to the Internet and in physical form. Important passwords should be stored not only digitally, but also in paper form, securely locked away.
  More information at: https://hilfe.uni-paderborn.de/Datensicherung (german)

- Do not operate with administrative rights when handling day-to-day matters. Create a user account within your operating system without administrative rights and use only this account for your work. This way, no software can be installed by the operating system without consulting you.

- Turn off macros in Office programs. Harmful software is often smuggled onto computers this way. If it is not mandatory for you to work with macros in your office software, disable them completely.

What to do if you are affected?

- Inform the information security team (informationssicherheit@uni-paderborn.de) and your environment about the issue. More information at: https://www.uni-paderborn.de/en/university/information-security

- Change all credentials stored and entered on the affected systems.

- Malicious programs sometimes cause far-reaching (security-relevant) changes within the infected system. After a forensic scan, you must reboot the computer yourself or have it rebooted by a professional.

Do you need help?
Contact your faculty's IT operations.

Faculty of Cultural Studies
IT support for employees of KW https://kw.uni-paderborn.de/en/fakultaet/it-support (german)

Faculty of Economics

IT-Administration of the Faculty of Economics
https://wiwi.uni-paderborn.de/en/fakultaet/organisation/fakultaetsverwaltung
(german)

Faculty of Natural Sciences

IT and IT Security Faculty of Natural Sciences
https://nw.uni-paderborn.de/en/fakultaet/organisation/it-and-it-security

Faculty of Mechanical
Engineering MB IT
https://mb.uni-paderborn.de/en/mb-it (german)

Department of Electrical Engineering, Computer
Science, and Mathematics
Computer Operations
https://cs.uni-paderborn.de/en/irb
Computer Operations Mathematics
https://math.uni-paderborn.de/en/rechnerbetrieb

Contact IMT User Services (imt@upb.de) with questions about software or IMT services.

Do you have any questions or suggestions regarding information security? Do not hesitate to contact the information security team (informationssicherheit@uni-paderborn.de).