UNIWERSYTET WARSZAWSKI

Data Protection Officer

IOD-042-04/2026

CYBER HYGIENE PRACTICES

A Cybersecurity Guide for the Academic Community of the University of Warsaw

Warsaw, 19 February 2026

I. Introduction

As digital technologies continue to evolve, data is now one of the most valuable assets for both organisations and individuals. In today's digital age, where information is constantly processed and shared, protecting it has become increasingly important. Every day, we process and exchange vast amounts of data – both in our private and professional lives. However, this also means a greater risk of **information security breaches**.

We store data in IT systems and email accounts, as well as in the cloud and on mobile devices. As the amount of data continues to grow, so too does the number of threats.

Cyber hygiene refers to everyday practices and habits that help reduce the risk of security breaches. It is not just about technology – it primarily depends on user awareness and responsible behaviour.

The aim of this guide is to present the key concepts, common threats and good practices related to data protection and digital security.

II. Basic terms and their definitions

Cybersecurity – a set of measures, technologies and procedures aimed at protecting systems and data from unauthorised access, loss or disruption.

Cyber hygiene – a set of good practices related to the safe use of information technology, including password management, system updates, data protection and vigilance against potential threats.

Data – any information recorded in any form that describes individuals, events, processes or work results, and that can be stored, processed and shared.

Among others, this includes:

- personal data (e.g. name, surname, email address);
- research data (e.g. measurement results, surveys, models, articles before publication);
- teaching data (e.g. course materials, grades);
- administrative and financial data (e.g. documents, contracts);
- technical data (e.g. system logs, user identifiers, configurations).

In a nutshell, data is information that describes something and has value – organisational, academic or legal – and therefore requires adequate protection and proper management.

Security breach – any event that may breach the confidentiality, integrity or availability of data or IT systems. However, not every breach means that an attack has been successful. It may simply be an attempted breach or a situation that poses a security risk.

Examples of security breaches include:

- unauthorised access to a system;
- loss or theft of a device;

- sending an email containing data to the wrong person;
- malware infection;
- disclosure of data on the internet;
- a suspicious phishing message;
- a system failure affecting access to data.

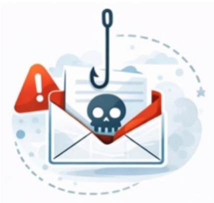
Security breaches may result in financial losses, operational disruption, reputational damage, legal consequences and the risk of identity theft.

It is worth noting that numerous breaches are caused by human error and unintended actions.

The **CIA** Triad – which stands for **confidentiality**, **integrity** and **availability** – is a framework that combines the three key principles of data protection: confidentiality (who can access the data), integrity (whether the data is accurate) and availability (whether the data can be accessed).

III. Common cybersecurity threats

Phishing



Phishing is a type of cyberattack that involves impersonating trusted institutions or individuals to obtain sensitive information, such as login credentials, personal data or financial information. Phishing attacks most often take the form of emails containing a link to a fake login page or an attachment containing malware.

The aim of phishing is to persuade the recipient to take action without careful verification, for example, by logging into a university system, confirming their details, downloading a file or making a payment. Fraudulent messages are often designed to appear credible and refer to current work-related matters.

Typical signs of phishing include:

- creating a sense of urgency or pressure to act immediately;
- requests to provide information, make a payment or click on a link;
- a slightly altered email address that looks legitimate;
- messages that play on fear, urgency or the consequences of not responding.

If you suspect phishing, do not click on any links or open any attachments. Instead, verify the message through an official communication channel or contact your IT department.

Further information is available on the following websites:
https://odo.uw.edu.pl/2025/05/09/uwaga-phishing-komunikat-iod/
https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/07/Phishing.pdf
https://cert.pl/posts/2025/09/analiza-adresow-stron/
https://cert.pl/posts/2023/04/phishing-webmail/

Malware

Malware (malicious software) is any program or code that is installed on a device without the user's knowledge or consent, with the aim of compromising the security of the system or data. Malware can operate in the background, collect information, disrupt a computer's performance or enable further attacks.

The most common functions of malicious software include stealing login credentials, monitoring user activity, taking control of a device, encrypting files, and using it to send spam or launch attacks on other systems.

Malware infection may occur, for example, after opening a suspicious attachment, clicking on a malicious link, installing unauthorised software or connecting an infected storage device. Malware can lead to data breaches, loss of research results, or disruption to e-learning and administrative systems.

Protection against malware relies on keeping software up to date, using security tools, being cautious with files and links, and limiting software installations to trusted sources.

Ransomware

Ransomware is a type of malicious software that blocks access to data or encrypts files and then demands a ransom to restore access. After a ransomware infection, users often cannot open their documents, and a ransom note demanding payment appears on the screen.

Ransomware attacks may begin with clicking on a malicious attachment or phishing link, installing unauthorised software or exploiting outdated software. In a university environment, ransomware can block access to teaching materials, research results, project documentation or administrative systems, seriously disrupting operations.

Paying the ransom does not guarantee data recovery and may encourage attackers to carry out further attacks. Therefore, **prevention is essential**: keeping software up to date, being cautious with messages and links, limiting user privileges, and creating backups that allow data to be restored without paying the ransom.

Further information is available on the following website:
https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Smishing (SMS phishing)

Smishing is a type of cyberattack that involves obtaining sensitive information through text messages or messaging apps. The attacker sends a message while impersonating a trusted institution, such as a delivery service, bank, payment service provider, or university system administrator.

The message typically claims that an additional payment is required for a parcel, that an account has been blocked, that urgent verification is needed, or that the recipient has won a prize. Its aim is to persuade the recipient to click on a link to a fake website, where they are asked to enter login credentials, personal data or payment information.

The fundamental security principle is to avoid clicking on links in unexpected messages and to verify information directly on your institution's official website or by contacting the IT department. Messages that create a sense of urgency or require immediate action should be treated with the utmost caution.

Further information is available on the following website:
https://cert.pl/baza-wiedzy/falszywe-smsy/

Vishing (voice phishing)

Vishing is a type of cyberattack that uses telephone calls. The caller impersonates a trusted institution or colleague - for example, a bank employee, IT staff member, courier, IT service provider or supervisor – and tries to persuade the recipient to disclose information or take a specific action.

Vishing may aim to obtain login credentials, authorisation codes or information about university systems, persuade the victim to install software, or trick them into making a bank transfer. Attackers often create a sense of urgency, invoke authority (e.g. "security department" or "an urgent matter from your manager") or warn of negative consequences to prompt quick action without proper verification.

The fundamental security principle is to adopt a limited trust approach: sensitive data, passwords and authorisation codes should **never** be shared over the phone. If a request seems unusual, end the call and contact the person or department directly using an official communication channel.

Further information is available on the following website:
https://odo.uw.edu.pl/2025/05/15/uwaga-vishing-komunikat-iod/

IV. Fundamental principles of cyber hygiene

Keep your software up to date and use trusted security tools

Regular updates of operating systems, applications and antivirus software eliminate identified security vulnerabilities and significantly reduce the risk of security breaches. Don't put off any updates, as many attacks exploit known, unpatched vulnerabilities.

Use strong, unique passwords and enable two-factor authentication (2FA)

Passwords should be long, unique and difficult to guess. Using the same password across multiple services is not recommended. Use a password manager and enable two-factor authentication wherever possible.

Recommended reading - guides:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/03/praca-zdalna-poradnik.pdf
https://cert.pl/bezpieczne-hasla/

Protect information from unauthorised access

Whenever you leave your workstation, lock your computer screen. You should also ensure the confidentiality of both paper and electronic documents and avoid leaving storage devices unattended.

Recommended reading - guide:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/03/bezpieczne-korzystanie-z-urz%C4%85dze%C5%84-IT.pdf

Use only secure connections and trusted devices

When working remotely, use the university VPN and a secure Wi-Fi network. Avoid logging into work systems from public, unsecured networks and installing unauthorised software on work devices.

Recommended reading - guide:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2021/02/DOZI.W.01.2021.pdf

Share information only with authorised persons

Apply the principle of least privilege: share data only with those who need it to carry out their work responsibilities. Before sending a message, always check that the recipient's address is correct, especially when the correspondence contains sensitive data.

Be cautious with messages and links

Be cautious of unusual emails, especially those containing requests for urgent action, language errors or suspicious attachments. Before clicking on a link or opening a file, verify the sender. If in doubt, contact the IT department.

Recommended reading - guides:

https://odo.uw.edu.pl/2025/05/30/jak-bezpiecznie-korzystac-z-poczty-elektronicznej/
https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/12/wskazowki-dot.-prowadzenia-korespondencji.pdf
https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf

Be mindful of what you share online

When sharing information online, be mindful of what you post. Avoid publishing details that could help attackers exploit vulnerabilities, such as information about infrastructure, procedures or schedules.

Encrypt data and portable storage devices

When working with sensitive data, encrypt all files and secure all external storage devices, such as USB drives and portable hard drives. The loss of an unsecured device may result in a data security breach.

Create backups regularly

It is recommended to create backup copies of important files and documents. Backups should be stored in a secure location and periodically tested to ensure that data can be successfully restored.

Participate in trainings regularly

Participate in trainings and stay up to date with security notices and guidance.

Trainings: https://odo.uw.edu.pl/szkolenia/

Report security breaches immediately

Any suspected security breach, such as a lost device, suspicious login activity or unauthorised access to data, must be reported immediately to the appropriate department. Early reporting helps minimise the potential impact and limit possible damage.

Reporting security breaches: https://odo.uw.edu.pl/zglaszanie-naruszen-ochrony-danych/

email address: **iod@adm.uw.edu.pl**