Educating Talents
since 1460.

University of Basel
Petersplatz 1
P.O. Box 2148
4001 Basel
Switzerland

www.unibas.ch

University of Basel

Getting started with **digital security**

Educational Technologies | **Project Digital Literacies**
More information: https://digitalskills.unibas.ch
Contact: digital-literacies@unibas.ch

Version of this document: 1.0, August 2023

This document has been authored
by the Team Educational Technologies
of the University of Basel.

This document is licensed under the license:
Creative Commons Attribution–Non-Commercial–ShareAlike 4.0 International
https://creativecommons.org/licenses/by-nc-sa/4.0/

The logo of the University of Basel is under copyright.

Getting started with digital security

Security breach, data loss or identity theft are dangers that are easily underestimated. And yet, digital security should be everyone's concern, especially in large organizations, since compromised personal accounts can be used to infiltrate organization's digital infrastructure, for instance to retrieve confidential information or for financial gain.

Luckily, good security practice is nothing complex for the end-user. It can be summarized in a few rules that are presented in this document.

Moreover, as it is easier to follow a rule when its purpose is understood, this brochure provides information not only about the “how”, but also about the “why” of digital security.

1

Manage your passwords wisely

- ✓ Use only strong passwords for all your logins
- ✓ Do not use the same password twice
- ✓ Use a password manager – a dedicated password manager is safer than other methods (e. g. using your web browser)
- ✓ If available, make sure to use two-factor authentication
- ✓ Enable the lock screen function on all your devices, and set up your computer to lock automatically when not in use

Explanations

As everyone knows from everyday experience, a user name and a password are required to log into the system of a company or organisation and use its services. This of course also applies to the University of Basel (details can be found on the Access web page of the IT Services).

A password is attributed upon entering the organization, and then changed by the user. Password can be changed at any time through the viaweb online service. This must occur at least once a year.

To ensure password strength, certain criteria must be met. The University of Basel enforces the following rules (details are on this web page):

- at least 12 characters, including
- numbers,
- uppercase letters,
- lowercase letters,
- and symbols, such as: & _ : !

The reason behind this, as explained in this press article, is that computers can crack any password below six characters almost instantly. Due to so-called dictionary attacks, the same applies to any password made of recognisable words, regardless of length, even if the words are slightly altered (e.g. by using "0" instead of "O"). By contrast, well-crafted passwords require years or even decades for computers to crack.

Moreover, the University of Basel implements a **two-factor authentication system** (details can be found on this ITS webpage): typically, a number is taken from an App and must be entered to complete the login process. The number can also be sent via SMS, but this is much less secure.

In this way, potential attackers attempting login need not only a password but also physical access to a specific device. Note that you should enable the lock screen function on mobile devices (in this area, passwords and face recognition are more secure than patterns and PIN codes). The same goes for your computer; in addition, activate the "autolock" function to make sure your computer locks on its own when you are away.

Lastly, it is crucial to have **different passwords** for each service. In this way, if one account is compromised, the other ones are still safe. Attackers know that many users do not follow this rule and typically try to login with the same credentials on a variety of platforms and services.

It is common to accumulate over time a very large number of login credentials. If the policy to use only unique strong passwords is applied consistently, it becomes impossible to know all credentials by heart.

This is where **password managers** come to the rescue: they store all passwords in an encrypted database. They can be set to autofill certain login forms. They can also generate random passwords and test for password strength. On the negative side of password managers, losing one's master password results in the loss of all credentials, with no possibility of recovery: for this reason, special care in this area is required.

Password managers exist as applications to install on one's device, such as the cross-platform, open source KeepassXC, or as online tools (such as the equally open source Bitwarden). The Data Protection Office of the Canton of Zurich provides a web page with advice on password managers.

Saving passwords in one's web browser is practical, but less secure than a special application dedicated to password management. You can increase security by using a strong master password in your browser and also restricting access to your device with a password, as indicated above.

2

Install updates regularly

- ✓ On your your private devices, install updates regularly for both your applications and for your operating system (Windows, iOS, Android, etc.)
- ✓ On your professional devices, install updates and upgrades when prompted: at the University of Basel, the IT Services communicate regularly about updates
- ✓ Choose your software wisely, taking security into account: you will find advice on the Software Literacy page of the Digital Skills portal of the University of Basel

Explanations

No software is flawless. This is true not only of features (that may be missing) or interfaces (that may be confusing). It is also true in the area of security: sometimes applications contain errors or weaknesses that attackers may exploit to steal data or breach into computing systems.

Software companies as well as individual programmers spend a lot of time ensuring that their applications are safe and secure. Also, security specialists regularly audit tools and report flaws.

As a result, programs regularly receive **updates**. In many cases, users can choose to have applications upgrade automatically in the background – this is the safest method (as opposed to downloading and installing the last version, which entails a small risk of retrieving the program from the wrong website).

Note, however, that all this is true only for tools that are in active development. The global software landscape changes rapidly and it is not uncommon for applications, including fairly popular ones, to be discontinued and sometimes even silently abandoned by their developers. Users who are software literate know about this and regularly check the status of the tools they rely on.

3

Pause and think

- ✓ Take your time when logging in and always make sure you are visiting the right page
- ✓ Be careful with e-mails from unknown senders; before clicking on links, double-check the destination by hovering over it with your mouse; treat attachment with suspicion, as they may contain malware
- ✓ Ignore any request for your password to be sent via e-mail or text message: serious organizations never ask sensitive information to be sent in this way
- ✓ Be careful when receiving urgent requests apparently sent by friends: this may be a case of impersonation; if unsure, reach out by calling or texting the person (avoid replying to the e-mail)
- ✓ Report phishing e-mails or, when unsure, ask for expert advice: at the University of Basel, this can be done by writing to the address phishing@unibas.ch

Explanations

So far we have dealt mostly with the technical side of digital security. Increasingly, however, attackers rely on so-called **social engineering** to manipulate users and have them either reveal their credentials, or unwillingly install unwanted software.

A common method consists in inviting users per e-mail to do a login on a fake website, for instance by way of fraudulent e-mails or text messages, with a view to harvest the user's credentials. In most cases, a fake sense of urgency is created (e.g. "act now to avoid losing access", "come pick up your order", "urgent unpaid bill" and even "security alert"). This is called **phishing**. Obviously, password strength offers no protection against this approach.

In the past, fraudulent e-mails and login pages often contained red flags such as bad spelling, funny grammar, and unusual layout – nowadays, however, due among other things to new tools based on artificial intelligence, text and layout may be almost perfect. Note that in up-to-date browsers the URL (address of the web page) cannot be faked: this is the thing to check when in doubt.

When checking the URL, be aware that it may be only minimally different from the one you are trying to access (for instance, www.unlbas.ch as opposed to www.unibas.ch).

Also, make sure to properly identify the domain. For instance,

- www.drive.example.ch belongs to example.ch
- but www.drive.example.ch.com belongs to ch.com

Another widespread social engineering technique next to phishing is **impersonation**: the account of a person you know may have been compromised, resulting in requests for help, especially in the form of money.

Sometimes messages are sent that contain so-called **malware**, i.e. malicious software: it is usually an attachment that, when opened, installs a program on the device, allowing the attacker to remotely control it. The goal is sometimes to steal data or in some cases to use the compromised computer as a platform for further malevolent activities (e.g. sending spam, generating clicks).

The installed program can also be so-called **ransomware**: it encrypts the attacked device and asks the user to pay a ransom to recover their data. Especially large organizations, including universities and hospitals, have been victims of such attacks in recent years. It is noteworthy that the point of attack was in many cases the account of a single member of the organization.

In rare cases, especially on mobile devices, simply clicking on a link, for instance in an SMS message, may be sufficient to have one's device compromised by malicious software.

The only way to defeat social engineering techniques is to **stay alert**: users must get into the habit of pausing and thinking before answering messages, clicking on links, opening attachments, or installing software.

When in doubt, it is best to abstain. If you realize you may have given your credentials to the wrong website or installed malicious software, make sure to contact your organization. At the University of Basel, write immediately to phishing@unibas.ch.

4

Backup frequently

- ✓ Do frequent backups, not only of your computer, but of your other devices as well
- ✓ To automatize the backup process, you can use tools such as the free and open source Duplicati or Time Machine (for Apple devices only)
- ✓ Consider the advantages and disadvantages of your backup destination (capacity, privacy, cost, etc.)

Explanations

The data stored on your devices or in the cloud may be compromised in many ways. Your computer or phone may get stolen. A hardware problem may render your data unavailable. The organization managing the cloud service may be facing problems. As explained above, your device may have been encrypted by so-called "ransomware". All these events can cause a complete loss of one's data.

The remedy against data loss of these unfortunate events is to have **recent backups**. This is part of the routine of organizations: for instance, the files stored on the network drives of the University of Basel, as well as the ones on the University's intranet, receive regular backups (as opposed to the files on your personal device, even if it is a managed one).

Frequent backups make a lot of sense for individuals as well. In most cases, your mobile device is backed up in the cloud. On your computer, by contrast, a backup routine must be set up manually.

For computers managed by the University of Basel, you can use the University's internal network drives (which, as mentioned, themselves receive backups). For your personal computer, consider which destination – cloud or external hard drive – is most appropriate for you.

Hard drives are typically more capacious and pose less data protection problems, but obviously require the extra step of physically attaching the device.

When choosing the cloud, the best practice is to encrypt your data beforehand, for instance with a tool like Cryptomator (available from the application's website – or alernatively, on managed devices, from the Portal Manager of the University of Basel).

For important data, it is also best practice to have not one, but two backups in two different locations (e.g. one in the cloud, one on an external hard drive).

Note that storage solutions like Google Drive or Dropbox are not ideal as backup tools. These tools synchronize between two different drives (basically, between your computer and the cloud): a problem on one drive (for instance, a file was deleted by mistake, or corrupted by a hardware failure) may thus propagate to other one. By contrast backups, to put it simply, are snapshots of data at a given time and do not change.

5

Get help and stay informed

If you are stuck or unsure about something pertaining to security, the IT Services the University of Basel are here to help. You can write to support-its@unibas.ch.

To deepen your understanding of digital security, you can use the resources below. Some of them are specific to the University of Basel, others come from other universities, still others apply more generally.

- **Security instructions of the IT Services**. The ITS have many webpages on security and data protection. It includes, among other things, a presentation of the general security rules, information on password security and on privacy and data protection. The present brochure uses the ITS pages as its source, but leaves out many details.
- **Digitally safe with SECUSO**. The SECUSO research group at the University of Karlsruhe has a website on digital privacy and security with tests, descriptions of best practices as well as recommendations for tools.
- **Security advice from UC Berkeley**. The University of California at Berkeley gives a very useful summary of the ten most important security habits.
- **Online security with iBarry**. The Swiss Internet Security Alliance is committed to promoting online security and data protection. Its website "iBarry" offers numerous useful recommendations and presents best practices in this area.