Educating Talents
since 1460.

Universität Basel
Petersplatz 1
Postfach 2148
4001 Basel
Schweiz

www.unibas.ch

Universität Basel

Einstieg in die **digitale Sicherheit**

Bildungstechnologien | Projekt Digital Literacies
Mehr Information: https://digitalskills.unibas.ch
Kontakt: digital-literacies@unibas.ch

Version dieses Dokuments: 1.0, August 2023

Dieses Dokument wurd vom Team Educational Technologies
der Universität Basel Basel verfasst.

Einstieg in die digitale Sicherheit

Im digitalen Raum lauern Gefahren wie Sicherheitslücken, Datenverlust oder Identitätsdiebstahl, die häufig unterschätzt werden. Umso wichtiger ist es, dass digitale Sicherheit ein Anliegen aller ist, besonders in grösseren Organisationen: Kompromittierte persönliche Konten können dazu genutzt werden, um in die digitale Infrastruktur einer Organisation einzudringen – z. B. mit dem Ziel, vertrauliche Informationen abzurufen oder finanziellen Gewinn zu erzielen.

Eine gute Sicherheitspraxis ist für die Endnutzer:innen glücklicherweise nicht kompliziert. Sie lässt sich in einigen wenigen Regeln zusammenfassen, die im vorliegenden Dokument vorgestellt werden.

Weil es einfacher ist, solche Regeln umzusetzen, wenn ihr Zweck verständlich ist, bietet diese Broschüre nicht nur Informationen über das «Wie», sondern auch über das «Warum» der digitalen Sicherheit.

1

Kluges Passwort-Management

- ✓ Verwenden Sie ausschliesslich starke Passwörter für Ihre Logins
- ✓ Nutzen Sie ein Passwort jeweils nur für ein Login anstatt für mehrere
- ✓ Sichern Sie Ihre Passwörter in einem Passwort-Manager – dies ist sicherer, als sie bspw. im Browser zu speichern
- ✓ Falls angeboten, verwenden Sie für Ihre Logins die Zwei-Faktor-Authentisierung
- ✓ Aktivieren Sie auf all Ihren Geräten die Bildschirmsperre und stellen Sie Ihren Computer so ein, dass er sich automatisch sperrt, wenn Sie ihn länger nicht nutzen

Erläuterungen

Wie wir aus dem Alltag wissen, sind ein Benutzer:innenname und ein Passwort üblicherweise Voraussetzung, um sich in das System eines Unternehmens oder einer Organisation einzuloggen und deren Dienste zu nutzen. Dies gilt auch für die Universität Basel (Details finden Sie auf der Zugangs-Webseite der Informatikdienste).

Ein Passwort wird jeweils beim Eintritt in die Organisation vergeben und kann danach jederzeit über den Online-Service viaweb geändert werden. Hierzu werden Sie mindestens einmal im Jahr aufgefordert.

Ein starkes Passwort charakterisiert sich durch bestimmte Kriterien. An der Universität Basel müssen folgende erfüllt sein (Details dazu finden Sie auf dieser ITS-Webseite):

- mindestens 12 Zeichen lang, darunter
- Zahlen,
- Grossbuchstaben,
- Kleinbuchstaben,
- und Symbole, wie z. B.: & _ : !

Der Grund dafür wird in diesem Presseartikel veranschaulicht: Computer können fast jedes Passwort mit weniger als sechs Zeichen in kürzester Zeit knacken. Aufgrund sogenannter Wörterbuch-Angriffe gilt dies auch für ein Passwort, das aus erkennbaren Wörtern besteht, unabhängig davon, wie lang es ist und selbst dann, wenn die Wörter leicht abgewandelt sind (z. B. durch Verwendung von «0» statt «O»). Im Gegensatz dazu benötigen Computer für sorgfältig ausgewählte Passwörter Jahre oder sogar Jahrzehnte, um sie zu knacken.

Darüber hinaus wendet die Universität Basel ein Zwei-Faktor-Authentisierungssystem an (Details dazu finden Sie auf der ITS-Webseite): Hierbei wird in der Regel eine Nummer von einer Authentisierungs-App abgefragt, die zur Anmeldung eingegeben werden muss. Die Nummer kann auch per SMS verschickt werden, was jedoch wesentlich unsicherer ist.

Auf diese Weise benötigen potenzielle Angreifer:innen, die versuchen, sich mit Ihren Login-Daten anzumelden, nicht nur ein Passwort, sondern auch physischen Zugang zu einem bestimmten Gerät.

Wir empfehlen Ihnen, bei mobilen Geräten die Bildschirmsperre zu aktivieren (wobei Passwörter und Gesichtserkennung sicherer sind als Muster und PIN-Codes). Das Gleiche gilt für Ihren Computer: Aktivieren Sie die Funktion der automatischen Sperre, damit sich Ihr Computer bei Ihrer Abwesenheit von selbst sperrt.

Letztlich ist es wichtig, dass Sie **für jeden Dienst ein anderes Passwort** verwenden. Auf diese Weise sind die anderen Konten auch dann noch geschützt, wenn eines Ihrer Konten kompromittiert wird. Angreifer:innen wissen, dass viele Benutzer:innen diese Regel nicht befolgen und versuchen daher oft, sich mit denselben Anmeldedaten bei einer Vielzahl von Plattformen und Diensten anzumelden.

Im Laufe der Zeit sammelt sich oft eine grosse Anzahl von Anmeldedaten an. Bei konsequenter Umsetzung der Regel, nur sichere und immer unterschiedliche Passwörter zu verwenden, wird es fast unmöglich, alle Anmeldedaten auswendig zu kennen. Hier kommen **Passwort-Manager** zum Einsatz: Sie speichern alle Passwörter in einer verschlüsselten Datenbank und können so eingestellt werden, dass sie bestimmte Anmeldeformulare automatisch ausfüllen. Weiter können sie auch Zufallspasswörter generieren und die Stärke Ihrer Passwörter testen.

Der Nachteil von Passwort-Managern ist allerdings, dass der Verlust des Hauptpassworts den Verlust aller darin gespeicherten Anmeldedaten zur Folge hat, ohne dass diese je wiederhergestellt werden können: Aus diesem Grund ist damit besondere Vorsicht geboten.

Passwort-Manager sind als Anwendungen verfügbar, die wie das plattformübergreifende, quelloffene KeepassXC auf dem eigenen Gerät installiert oder als Online-Tools (wie das ebenfalls quelloffene Bitwarden) genutzt werden können. Eine hilfreiche Webseite mit Hinweisen zu Passwort-Managern bietet die Datenschutzstelle des Kantons Zürich an.

Das Speichern von Passwörtern im Webbrowser ist praktisch, aber weniger sicher als die Verwendung einer speziellen Anwendung nur für das Passwort-Management. Sie können hier die Sicherheit erhöhen, indem Sie ein starkes Hauptpasswort in Ihrem Browser verwenden und, wie oben beschrieben, auch den Zugang zu Ihrem Gerät mit einem Passwort einschränken.

2

Regelmässige Updates

- ✓ Installieren Sie auf Ihren privaten Geräten regelmässig Updates, sowohl für Ihre Anwendungen als auch für Ihr Betriebssystem (Windows, iOS, Android, etc.)
- ✓ Installieren Sie auf Ihren geschäftlichen Geräten Updates und Upgrades umgehend, wenn Sie dazu aufgefordert werden: An der Universität Basel informieren die IT Services regelmässig über Updates.
- ✓ Wählen Sie Ihre Software sorgfältig und unter Berücksichtigung ihrer Sicherheit aus: Empfehlungen hierzu finden Sie auf der Seite Software Literacy des Webportals Digital Skills der Universität Basel

Erläuterungen

Keine Software ist perfekt. Das gilt nicht nur für Funktionen (die vielleicht fehlen) oder Interfaces (die verwirrend sein können), sondern auch für den Bereich der Sicherheit: Manchmal enthalten Anwendungen Fehler oder Schwachstellen, die Angreifer:innen ausnutzen können, um Daten zu stehlen oder in Computersysteme einzudringen.

Sowohl Softwareunternehmen als auch einzelne Programmierer:innen verbringen viel Zeit damit, sicherzustellen, dass ihre Anwendungen sicher sind. Ausserdem überprüfen Sicherheitsspezialisten regelmässig Tools und melden deren Schwachstellen.

Aus diesem Grund gibt es für Programme regelmässig **Aktualisierungen**. In vielen Fällen können Nutzer:innen auswählen, dass die Anwendungen automatisch im Hintergrund aktualisiert werden sollen – dies ist die sicherste Methode (im Gegensatz zum Herunterladen und Installieren der neuesten Version, bei dem ein kleines Risiko besteht, das Programm von einer falschen Website abzurufen).

Beachten Sie jedoch, dass all dies nur für Tools gilt, die sich in aktiver Entwicklung befinden. Die Software-Landschaft verändert sich schnell, und es ist nicht unüblich, dass Anwendungen, auch beliebte, von ihren Entwickler:innen nicht weiterentwickelt und manchmal sogar stillschweigend aufgegeben werden. Benutzer:innen, die sich mit Software auskennen, wissen das und überprüfen regelmässig den Status der Tools, auf die sie angewiesen sind.

3

Realitätschecks

- ✓ Nehmen Sie sich Zeit fürs Login und versichern Sie sich jeweils, dass Sie auf die richtige Webseite gelangt sind
- ✓ Seien Sie vorsichtig mit E-Mails von unbekannten Absendenden; überprüfen Sie die Zielseite von Links bevor Sie auf sie klicken durch Darüberfahren mit der Maus; gehen Sie kritisch mit Anhängen um, da sie Schadsoftware (Malware) enthalten können
- ✓ Ignorieren Sie jegliche Aufforderung, Ihr Passwort per E-Mail oder SMS zu teilen: seriöse Organisationen bitten nie um die Übermittlung sensibler Informationen auf diesem Wege
- ✓ Seien Sie wachsam, wenn Sie dringende Anfragen erhalten, die scheinbar von Freund:innen gesendet wurden: Es könnte sich um eine falsche Identität handeln; wenn Sie unsicher sind, rufen Sie die Person an oder kontaktieren Sie sie via SMS (vermeiden Sie es, auf die E-Mail zu antworten)
- ✓ Melden Sie Phishing-Mails oder holen Sie Expert:innen-Rat ein, wenn Sie unsicher sind: An der Universität Basel können Sie hierfür die Adresse phishing@unibas.ch kontaktieren

Erläuterungen

Bis jetzt haben wir uns hauptsächlich mit der technischen Seite der digitalen Sicherheit befasst. Zunehmend setzen Angreifer:innen jedoch auf das so genannte **Social Engineering**, um Nutzer:innen zu manipulieren und sie dazu zu bringen, entweder ihre Anmeldedaten preiszugeben oder unfreiwillig unerwünschte Software zu installieren.

Eine gängige Methode besteht darin, Nutzer:innen per E-Mail aufzufordern, sich auf einer gefälschten Website anzumelden, z. B. durch betrügerische E-Mails oder Textnachrichten, um die Anmeldedaten der Nutzer:innen abzufangen. In den meisten Fällen wird dabei Dringlichkeit vorgetäuscht (z. B. «handeln Sie jetzt, um Ihren Zugang nicht zu verlieren», «holen Sie Ihre Bestellung ab», «dringende unbezahlte Rechnung» und sogar «Sicherheitswarnung»). Dies wird als **Phishing** bezeichnet. Natürlich bietet die Stärke des Passworts keinen Schutz gegen diese Vorgehensweise.

In der Vergangenheit enthielten betrügerische E-Mails und Anmeldeseiten oft Warnzeichen wie schlechte Rechtschreibung, unpassende Grammatik und ein ungewöhnliches Layout – heutzutage können Text und Layout jedoch nahezu perfekt aussehen, unter anderem aufgrund neuer Tools, die auf künstlicher Intelligenz basieren. Beachten Sie, dass in modernen Browsern die URL (Adresse der Webseite) nicht gefälscht werden kann. Im Zweifelsfall ist die URL also ein guter Anhaltspunkt, um die Seriosität der Seite zu überprüfen.

Beachten Sie bei der Überprüfung der URL, dass sie sich möglicherweise nur geringfügig von der Seite unterscheidet, die Sie eigentlich aufrufen möchten (z. B. www.unlbas.ch anstatt www.unibas.ch).

Achten Sie zudem darauf, die Domain richtig zu identifizieren. Zum Beispiel gehört

- www.drive.example.ch zu example.ch,
- hingegen www.drive.example.ch.com zu ch.com

Ein anderes weitverbreitetes Vorgehen des Social Engineering neben dem Phishing ist die sogenannte **Impersonation**: Das Konto einer Ihnen bekannten Person kann kompromittiert worden sein, und Sie werden angeblich von ihr bspw. um Hilfe gebeten, insbesondere in Form von Geld.

Manchmal werden Nachrichten verschickt, die so genannte **Malware**, d. h. bösartige Software, enthalten: In der Regel handelt es sich dabei um einen Anhang, der, wenn er geöffnet wird, ein Programm auf dem Gerät installiert, das es den Angreifenden ermöglicht, es fernzusteuern. Ziel ist es manchmal, Daten zu stehlen oder in manchen Fällen den kompromittierten Computer als Plattform für weitere böswillige Aktivitäten zu nutzen (z. B. Versand von Spam, Generierung von Klicks).

Bei dem installierten Programm kann es sich auch um sogenannte **Ransomware** handeln: Sie verschlüsselt das angegriffene Gerät und fordert den/die Benutzer:in auf, ein Lösegeld zu zahlen, um die Daten wiederherzustellen. Vor allem grosse Organisationen, darunter auch Universitäten und Krankenhäuser, waren in den letzten Jahren oft Ziel solcher Angriffe. Bemerkenswert ist hierbei, dass der Angriffspunkt in vielen Fällen das Konto eines einzelnen Mitglieds der Organisation war.

In seltenen Fällen, vor allem bei mobilen Geräten, kann ein einfacher Klick auf einen Link, beispielsweise in einer SMS-Nachricht, ausreichen, um das eigene Gerät mit Schadsoftware zu infizieren.

Der einzige Weg, sich gegen Social-Engineering-Techniken zu schützen, besteht darin, **wachsam zu bleiben**: Benutzer:innen sollten sich angewöhnen, innezuhalten und nachzudenken, bevor sie auf Nachrichten antworten, auf Links klicken, Anhänge öffnen oder Software installieren.

Im Zweifelsfall ist es am besten, solche Inhalte zu meiden. Wenn Sie feststellen, dass Sie Ihre Anmeldedaten an die falsche Website weitergegeben oder bösartige Software installiert haben, kontaktieren Sie Ihre Organisation. An der Universität Basel sind Sie angehalten, sich umgehend an phishing@unibas.ch zu wenden.

4

Regelmässige Backups

- ✓ Erstellen Sie regelmässig Backups, nicht nur von den Daten auf Ihrem Computer, sondern auch auf Ihren anderen Geräten
- ✓ Um den Backup-Prozess zu automatisieren, können Sie Tools wie das kostenlose und quelloffene Duplicati oder Time Machine (nur für Apple-Geräte) nutzen
- ✓ Ermitteln Sie die Vor- und Nachteile Ihres Speicherortes (Kapazität, Datenschutz, Kosten, usw.)

Erläuterungen

Die auf Ihren Geräten oder in einer Cloud gespeicherten Daten können auf vielerlei Weise kompromittiert werden. Ihr Computer oder Telefon kann gestohlen werden. Ein Hardware-Problem kann dazu führen, dass Ihre Daten nicht mehr verfügbar sind. Das Unternehmen, das den Cloud-Dienst verwaltet, könnte mit Problemen zu kämpfen haben. Wie oben erwähnt, kann Ihr Gerät auch durch sogenannte «Ransomware» verschlüsselt worden sein. All dies kann zu einem totalen oder vorübergehenden Datenverlust führen.

Die beste Massnahme zur Prävention von Datenverlusten ist die Erstellung **aktueller Backups**. In Organisationen ist dies Teil der Routine: Die Dateien auf den Netzlaufwerken der Universität Basel zum Beispiel sowie die Dateien im Intranet der Universität werden regelmässig gesichert (im Gegensatz zu den Dateien auf Ihrem persönlichen Gerät, selbst wenn es sich um ein verwaltetes Gerät handelt).

Regelmässige Backups sind auch für Privatpersonen sehr sinnvoll. In den meisten Fällen wird Ihr mobiles Gerät in der Cloud gesichert. Auf Ihrem privaten Computer hingegen muss eine Sicherungsroutine manuell eingerichtet werden.

Für Computer, die von der Universität Basel verwaltet werden, können Sie die universitätsinternen Netzlaufwerke der Universität verwenden (die, wie erwähnt, selbst Backups erhalten). Wägen Sie für Ihren persönlichen Computer ab, welches Speicherziel – Cloud oder externe Festplatte – für Sie am besten geeignet ist.

Festplatten haben in der Regel eine grössere Speicherkapazität und stellen weniger Probleme für den Datenschutz dar, erfordern aber natürlich den zusätzlichen Schritt, das Gerät physisch anzuschliessen.

Wenn Sie sich für die Cloud entscheiden, verschlüsseln Sie Ihre Daten am besten vorher, zum Beispiel mit einem Tool wie Cryptomator (erhältlich beim Portal Manager der Universität Basel).

Für wichtige Daten empfiehlt es sich auch, nicht nur ein, sondern zwei Backups an zwei verschiedenen Stellen zu haben (z. B. eines in der Cloud und eines auf einer externen Festplatte).

Beachten Sie, dass Speicherlösungen wie Google Drive oder Dropbox als Backup-Tools nicht ideal sind. Diese Tools synchronisieren nämlich zwischen zwei verschiedenen Laufwerken (zwischen Ihrem Computer und der Cloud): ein Problem auf der einen Seite (z. B. eine Datei wurde versehentlich gelöscht oder durch einen Hardwarefehler beschädigt) kann sich auf der anderen Seite propagieren. Vereinfacht gesagt sind Backups, im Gegensatz dazu, Schnappschüsse von Daten zu einem bestimmten Zeitpunkt und ändern sich nicht.

5

Hilfe erhalten und informiert bleiben

Wenn Sie nicht weiterkommen oder unsicher sind, was das Thema Sicherheit betrifft, helfen Ihnen die Informatikdienste der Universität Basel weiter. Sie können sich jederzeit an support-its@unibas.ch wenden.

Um Ihr Verständnis von digitaler Sicherheit zu vertiefen, können Sie die untenstehenden Ressourcen nutzen. Einige darunter sind spezifisch für die Universität Basel, andere stammen von anderen Universitäten, wieder andere gelten allgemeiner.

- **Sicherheitshinweise der IT-Services**. Die ITS bieten mehrere Webseiten zum Thema Sicherheit und Datenschutz. Sie enthalten unter anderem eine Darstellung der allgemeinen Sicherheitsregeln, Informationen zur Passwortsicherheit und zum Schutz der Privatsphäre und des Datenschutzes. Die vorliegende Broschüre nutzt die Seiten des ITS als Quelle, lässt aber viele Details weg.
- **Digital sicher mit SECUSO**. Die SECUSO-Forschungsgruppe der Universität Karlsruhe hat eine Website zum Thema digitale Privatsphäre und Sicherheit mit Tests, Beschreibungen bewährter Verfahren sowie Empfehlungen für Tools.
- **Sicherheitstipps der UC Berkeley**. Die Universität von Kalifornien in Berkeley bietet eine nützliche Zusammenfassung der zehn wichtigsten Sicherheitsgewohnheiten.
- **Online-Sicherheit mit iBarry**. Die «Swiss Internet Security Alliance» setzt sich für die Förderung der Internet-Sicherheit und des Datenschutzes ein. Ihre Website "iBarry" bietet zahlreiche nützliche Empfehlungen und stellt Best Practices in diesem Bereich vor.