

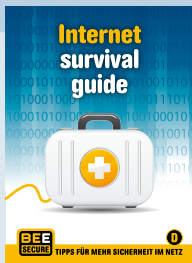
# Internet survival guide



**BEE**  
**SECURE**



**TIPPS FÜR MEHR SICHERHEIT IM NETZ**



Dieser Leitfaden richtet sich an SchülerInnen und Studierende mit Ratschlägen, Tipps und Tricks um ihre Hardware sowie ihre Daten zu schützen. Die Informationen können für alle, die ihre Daten und ihre Privatsphäre schützen möchten, nützlich sein.

Ein Rechner ist leicht ersetzbar, eine verloren gegangene Studienarbeit dagegen nur schwer.



*Es wird darauf hingewiesen, dass alle Angaben in diesem Booklet trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der AutorInnen ausgeschlossen ist.*



**Herausgeber : SNJ**

Annexe Forum Geesseknäppchen  
40, bld. Pierre Dupong  
L-1430 Luxembourg  
B.P. 707 - L-2017 Luxembourg

info@bee-secure.lu  
www.bee-secure.lu



Service National  
de la Jeunesse



SECURITY  
MADEIN.LU



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG



Cofinanced by the European Union  
Connecting Europe Facility

Unveränderte nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt unter Angabe der Quelle.



Consultez :  
<http://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>

**Rechtlicher Hinweis**

Dieses Booklet wurde im Rahmen des Projekts BEE SECURE produziert.

Das Projekt wird gemeinsam vom Service National de la Jeunesse (SNJ), dem KannerJugendTelefon (KJT) und securitymadein.lu umgesetzt.

# 1) Die physikalische Sicherheit

Um deine Daten zu schützen, musst du zuerst deine Geräte (Tablet, PC, Harddisk, USB-Stick, ....) schützen:

- Lass deine Geräte niemals unbeaufsichtigt. Laptops, die an öffentlichen Orten benutzt werden, sollten mit einem Antidiebstahl-Kabel gesichert werden.
- Wenn du dein Gerät trotzdem unbeaufsichtigt lassen musst, aktiviere immer vorher die Bildschirmsperre. Vergewissere dich ebenfalls, dass dein Gerät mit einem Passwort, einem PIN-Code, Gesichtserkennung, oder mit einem Fingerabdruck gesichert ist.
- Verschlüssele wenn möglich deine Festplatte und deine Backups und bewahre die Sicherheitskopien so auf, dass sie nicht direkt zugänglich sind.
- Lass deine USB-Sticks und SD-Karten nicht herumliegen, wenn du darauf Dokumente aufbewahrst. Benutze nie unbekannte USB-Sticks, diese können mit Schadprogrammen (Malware) infiziert sein.

## Daten verschlüsseln:

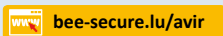
Alle modernen Betriebssysteme bieten die Möglichkeit, Daten auf der Festplatte zu verschlüsseln: „**Bitlocker**“ unter Microsoft Windows oder „**FileVault**“ unter Apple OS X.

Es gibt auch unabhängige Tools, die unter allen Betriebssystemen laufen, zum Beispiel Boxcryptor, DiskCryptor, VeraCrypt... Diese erlauben dir auch deine Daten in der Cloud zu verschlüsseln und über verschiedene Geräte darauf zuzugreifen. Download auf:



## 2) Konfiguration des Systems

- **Benutzerkonten:** Verwende nicht ständig ein Konto mit Administrator-Rechten, sondern ein „eingeschränktes“, passwortgeschütztes Benutzerkonto, wenn du im Internet surfst, spielst oder arbeitest. Aktiviere bei Bildschirmschonern oder dem Stromspar-Modus die Passwortabfrage.
- **Root/Jailbreak** erlauben Apps, erweiterte Systemeinstellungen vorzunehmen (z.B. Standard-Apps zu löschen, oder System-speicher freizugeben). Dies erlaubt aber auch böartigen Apps, Sicherheitsmechanismen auszuhebeln und die Kontrolle über das gesamte Gerät zu übernehmen. So können sie z.B. sensible Daten (Passwörter, Bankdaten) auslesen. Root/Jailbreak sollte daher unter allen Umständen vermieden werden.
- **Updates:** Vergewissere dich, dass alle Apps und Programme auf deinen Geräten automatisch aktualisiert werden. Auf Geräten, wo es keine automatische Update-Funktion gibt (wie bspw. auf Fernsehern, oder sonstigen „smarten“ Geräten), überprüfe regelmäßig die Webseiten der Anbieter auf neue Versionen.
- **Anti-virus:** Installiere ein Antivirenprogramm, das, wenn möglich täglich, automatisch aktualisiert wird. Kostenlose Lösungen findest du hier:



Scanne regelmäßig deinen Computer nach Malware. Verlasse dich nur auf Warnungen deines eigenen Antiviren-Programms und ignoriere Warnungen, dass dein Computer infiziert sei, die du via Internet oder E-Mail erhältst.

- **Sicherheitskopien (Backup):** Verwende die Backup-Funktionen deines Betriebssystems. Speichere deine Sicherheitskopien möglichst verschlüsselt auf externen Festplatten und/oder in der Cloud.

- **Berechtigungen:** Wenn du eine App herunterlädst, überprüfe, ob diese App auf deine Kamera, dein Mikrofon, dein Standort, deine Kontakte oder sonstige Daten zugreifen, und ob sie kostenpflichtige Anrufe tätigen darf. Entziehe ggf. diese Berechtigung in den Systemeinstellungen, oder deinstalliere die App komplett.

## Web-Browser:

Da Erweiterungen oft der Grund für unbeabsichtigte Werbung sind, sollten unnötige Erweiterungen vermieden werden. Überprüfe daher auch regelmäßig, welche Erweiterungen ohne dein Zutun installiert wurden. Die Verwendung folgender Erweiterungen wird allerdings empfohlen:

- **NoScript** verhindert die Ausführung von potenziell bösartigen Skripten, hat jedoch negative Auswirkungen auf den Komfort bei der Browser-Benutzung:



[bee-secure.lu/nosc](https://bee-secure.lu/nosc)

- **https everywhere:** Die Kommunikation mit dem Server erfolgt wenn möglich verschlüsselt:



[eff.org/HTTPS-everywhere](https://eff.org/HTTPS-everywhere)

- **Flashblock**, (nicht nötig, falls bereits NoScript installiert ist). Inhalte für Adobe Flash, welche häufig Angriffsflächen bieten, werden unterbunden:



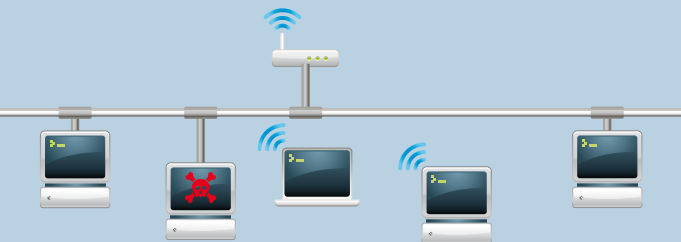
[bee-secure.lu/flbl](https://bee-secure.lu/flbl)

- **Adblocker** blockieren Werbung, Fake-Meldungen, und nervige Pop-ups auf Internetseiten und in Videos.

- **Drahtlose Netzwerke (WiFi):** Sichere deinen drahtlosen Zugangspunkt (WiFi-Router) zuhause mittels WPA2-Verschlüsselung und ändere regelmäßig das Passwort. Deaktiviere die Fernsteuerungsfunktion des Routers, wenn du sie nicht nutzt.

Benutze in der Schule oder an der Uni nur die speziell für den Unterrichtszwecke eingerichteten Zugänge (WiFi der Schule, EduROAM) wenn diese verfügbar sind. Sie bieten dir einen gesicherten Internetzugang und, wenn nötig, kannst du auf einen Helpdesk-Dienst zurückgreifen.

- **Öffentliche Netzwerke:** Benutze unbekannte oder öffentliche Netzwerke nur, wenn unbedingt nötig, da sie Hackern die Möglichkeit bieten, alles mitzulesen, was du tust. Benutze in solchen Netzwerken nur verschlüsselte Verbindungen, wenn du im Internet surfst (achte auf HTTPS) oder deine E-Mail abrufst (achte auf TLS/SSL in den Einstellungen). Messenger, WhatsApp, Snapchat und Co. sind in der Regel entsprechend abgesichert, sodass du sie ohne Bedenken nutzen kannst. Vermeide hingegen sicherheitsbedenkliche Aktionen wie Anmeldungen, Eingabe von sensiblen Daten, oder Onlinekäufe.
- **Bluetooth:** Bei Nichtgebrauch ausschalten.
- **Datenfreigabe, Lokalisierung und NFC:** Deaktiviere die gemeinsame Nutzung von Daten und Ressourcen (Internetzugang, Festplatten, Drucker, usw.), sobald diese nicht mehr benötigt wird.



### 3) Passwörter

**Passwörter sind der Schlüssel zu Deiner digitalen Sicherheit.**

Verwende lange Passwörter (mehr als 12 Zeichen) oder noch besser „Passsätze“, bestehend aus Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

**Das Passwort sollte nicht:**

- in einem Wörterbuch stehen;
- auf persönlichen Angaben basieren (Name, Geburtsdatum, usw.);
- eine logische Zahlen- oder Buchstabenfolge sein (123456, abcdef...).

**Wähle unterschiedliche Passwörter** für die verschiedenen Online-Dienste die du nutzt. So vermeidest du, dass der Zugang zu allen Konten offen ist, falls das Passwort unabsichtlich oder gar mit bösen Absichten offengelegt wird.

**Aktiviere die doppelte Authentifizierung** wenn immer dies möglich ist.

Ersetze stets die Standard-Passwörter und teile niemandem Deine Passwörter mit.

**Passwörter  
sind wie Zahnbürsten.  
Man sollte sie nicht teilen.**



## Wahl eines Passworts:

Suche dir einen einprägsamen Satz aus, beispielsweise „Ziehen sie voll Mörderdrang Niep und Piep die Hälse lang!“ (Wilhelm Busch). Nimmt man von jedem Wort den ersten Buchstaben, so erhält man: „ZsvMNUdHl!“. Durch das Ersetzen einiger Zeichen mit Ziffern entsteht anschließend: „Z5vMNUdH1!“.

Alternativ kann man auch den gesamten Satz direkt als Passwort wählen. Hier sollte man allerdings drauf achten, dass der gewählte Satz nicht zu bekannt (man sollte also Sprichwörter u.ä. vermeiden) oder zu offensichtlich ist („ich heiße ...“).

Im Allgemeinen gilt: je kreativer und einzigartiger dein Passwort, desto sicherer ist es

Teste dein Passwort:



[pwdtest.bee-secure.lu](https://pwdtest.bee-secure.lu)

## Passwörter verwalten

Unterschiedliche und trotzdem sichere Passwörter für jeden einzelnen Online-Dienst zu verwenden kann schwierig werden, besonders wenn man viele davon nutzt. Um dem entgegenzuwirken kann man zum Beispiel ein sehr starkes Passwort wählen und es in verschiedenen Varianten verwenden (bspw. den Online-Dienst als Prä- oder Suffix ergänzen: „FB:ZsvMNUdHl!“ mit FB für Facebook) und/oder einen Passwortverwalter nutzen, wie zum Beispiel LastPass oder KeePass.



[bee-secure.lu/keep](https://bee-secure.lu/keep)

Mit diesen Tools kann man so viele Passwörter wie nötig speichern und starke Passwörter generieren. Außerdem warnen sie vor möglichen Sicherheitslücken der verwendeten Online-Dienste.

Ein Passwortverwalter schützt dich auch vor Phishing-Versuchen, die sichere Seiten von den Fälschungen unterscheiden kann, die dein Passwort stehlen wollen. Beachte, dass du für diese Funktion eine Browser-Erweiterung installieren musst.



**Achtung:** ein Passwortverwalter funktioniert wie ein Safe. Wenn du alle deine Passwörter darin speicherst, muss der Safeschlüssel sehr sicher sein und darf auf keinen Fall bekannt werden oder verloren gehen. Aktiviere die doppelte Authentifizierung bei deinem Passwortverwalter.

## 4) Verhaltensregeln

### Sei wachsam!

Sei misstrauisch und hüte dich vor Betrug im Internet. Dein Verhalten hat direkte Auswirkungen auf die Sicherheit deiner Daten.



### Surfen im Internet:

- Vermeide es unter allen Umständen, auf fremden Rechnern dein Passwort oder andere persönliche Daten einzugeben (insbesondere bei Einkäufen oder Bankgeschäften).
- Wenn du trotzdem ein Passwort auf einem fremden Rechner eingeben musst, verwende die „Private Browsing“- Funktion (Strg+Shift+P unter Firefox oder Internet Explorer, Strg+Shift+N unter Chrome) – weder dein Passwort noch andere personenbezogene Daten werden dann gespeichert. Die Benutzung einer virtuellen Tastatur (On-Screen Keyboard) ist ebenfalls anzuraten.
- Kontrolliere generell, ob „https“ (SSL-gesicherte Seite) am Anfang der Adresszeile des Browsers steht, bevor du sensible Daten wie Passwörter eingibst. Falls der Browser eine Warnung anzeigt, dass das Zertifikat einer SSL-gesicherten Seite ungültig ist, verlasse die Webseite ohne irgendwelche Transaktionen zu tätigen.

- Selbst der einfache Besuch bestimmter Websites kann durch das sogenannte „drive-by-download“ eine Infektion deines Systems verursachen. Vermeide daher Websites, denen du nicht absolut vertraust. Vermeide es ebenfalls, auf Werbungen zu klicken und auf Links in E-Mails. Software, wie bspw. Sandboxie oder Adblocker, kann dir beim Schutz deines Systems helfen.



**bee-secure.lu/sand**

Auch das Einschränken deiner Administratorrechte beugt Virusinfektionen vor.

## **E-Mails oder Textnachrichten:**

- Beantworte niemals E-Mails, die vertrauliche Informationen erfragen (z.B. Passwörter, Kontonummern, Kreditkartendaten usw.).
- Öffne niemals Links oder Anhänge, falls du deren Herkunft nicht mit absoluter Gewissheit kennst.
- Prüfe jede eingehende Nachricht kritisch bevor du handelst, auch wenn die Nachricht von einer dir bekannten Person stammt:
  - ☐ Ist die Nachricht irgendwie komisch? Unerwartet?
  - ☐ Ist die Sprache ungewöhnlich?
  - ☐ Ist es ein Hilferuf?
  - ☐ Schlägt die Nachricht dir vor an einem Wettbewerb teilzunehmen? Von einem Glücksfall zu profitieren?
  - ☐ Enthält die Nachricht einen Link oder einen Anhang?

Wenn die Antwort auf eine dieser Fragen positiv ist, sei vorsichtig und versuch auf anderem Wege mit der Person Kontakt aufzunehmen.

- Sei dir bewusst, dass eine E-Mail-Adresse leicht gefälscht werden kann.

## **Spam:**

- Um Spam zu vermeiden, nutze zwei E-Mail Adressen:

- eine Hauptadresse für vertrauenswürdige Empfänger,
- eine zweite Adresse (also eine Alias-Adresse) für öffentliche Kontakte.

Denk auch an die Möglichkeit von Wegwerf-E-Mails für nicht persönliche Daten:



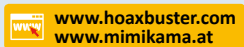
- Teile deine E-Mail-Adresse nicht bei jeder Gelegenheit mit und vermeide es, diese an öffentlich zugänglichen Bereichen anzugeben (Facebook, Blog, Flyer, usw.)
- Antworte unter keinen Umständen auf Spam.

## Hoaxes:

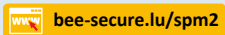
Vermeide es, Hoaxes, Falschmeldungen oder Fehlinformationen weiterzuleiten und bedenke:

- Vor Computerviren wird nie offiziell per E-Mail oder Textnachricht gewarnt.
- Sicherheits-Updates werden nie via E-Mail oder Textnachricht verschickt.
- E-Mails oder Textnachrichten mit der Bitte, die Nachricht an alle deine Kontakte weiterzuleiten (Kettenbriefe), sind fast immer Hoaxes oder Betrügereien.

Im Zweifelsfall, überprüfe die erhaltenen Informationen:



Kurz gesagt, lerne verdächtige E-Mails zu erkennen:



Um in jeder Situation clever zu klicken, befolge die Ratschläge von BEE SECURE:



## Soziale Netzwerke und Datenschutz:

- Beschränke die Verbreitung personenbezogener Informationen im Netz weitest möglich. Nimm dir Zeit, die Einstellungen deines Profils entsprechend sicher anzupassen.
- Vermeide es, private Fotos auf sozialen Netzwerken (Facebook, Snapchat, Instagram usw.) zu veröffentlichen. Sobald deine Daten veröffentlicht sind, verlierst du die Kontrolle darüber. Du solltest nur das online veröffentlichen, was du auch in eine Zeitung setzen würdest.
- Bitte Personen, die auf deinen Fotos abgebildet sind, um ihr Einverständnis bevor du sie veröffentlichst. Die Gesetze zum Recht am eigenen Bild gelten in Luxemburg sowie in anderen Ländern.

Kleine Erinnerung zum Recht am eigenen Bild:



[bee-secure.lu/cprt](https://bee-secure.lu/cprt)

- Stell dir folgende Fragen bevor du Inhalte auf sozialen Netzwerken teilst:
  - ☐ Ist der Text oder das Bild lizenzfrei?
  - ☐ Haben die Personen auf den Bildern deren Veröffentlichung zugestimmt?
  - ☐ Ist die Nachricht weder diffamierend, noch verleumderisch, diskriminierend oder gehässig?
  - ☐ Entspricht die Nachricht den allgemeinen Nutzungsbedingungen des Online-Diensts?

Ratschläge und Tipps zu Facebook:



[bee-secure.lu/fcbk](https://bee-secure.lu/fcbk)

Egal in welcher Stimmung du gerade bist, bleib fair.  
Mobbing ist kein Spiel:



[bee-secure.lu/beefair](https://bee-secure.lu/beefair)



## 5) Rechtliche Aspekte

### Handle verantwortungsvoll!

Du bist nicht anonym im Netz...  
und das Gesetz gilt auch im Internet:



[bee-secure.lu/lois](http://bee-secure.lu/lois)

Sei vorsichtig beim Verfassen von Texten oder Kommentaren oder beim Veröffentlichen von Fotos oder Videos im Netz – die Gesetzgebung zu Diffamierung, Verleumdung und dem Recht am eigenen Bild ist anwendbar.

**Als Zeuge von Mobbing** musst du eingreifen sonst bist du mitverantwortlich. Du kannst zum Beispiel diffamierende oder unangemessene Inhalte auf der betreffenden Seite melden. Oft hört Mobbing auf, wenn der Drahtzieher merkt, dass das Opfer nicht alleine ist.

**Als Opfer von Mobbing**, könnten dir diese Verhaltensweisen helfen:

1. Antworte unter keinen Umständen auf Belästigungen oder Bedrohungen
2. Blockiere deine Angreifer
3. Bewahre Beweise auf (z.B. Screenshots)
4. Melde die Vorfälle den Verantwortlichen der Seite oder des sozialen Netzwerks
5. Ändere deine Daten im Netz

Mehr Informationen zu diesem Thema  
findest du bei « Not funny - Bee fair »  
von BEE SECURE.



[bee-secure.lu/beefair](http://bee-secure.lu/beefair)

**NOT FUNNY**  
**BEE FAIR**

## So steht's im Gesetz...

**Beleidigung:** bei einer Beleidigung handelt es sich um eine Verletzung der Ehre, die gemäß dem Strafgesetzbuch mit einer Freiheitsstrafe zwischen 8 Tagen und 2 Monaten geahndet werden kann, sowie mit einem Bußgeld von bis zu 5000 Euro oder mit nur einer dieser beiden Strafen.

**Verletzung der Privatsphäre:** dieses Recht ist im Gesetz des 11/08/1982 verankert, sowie in Artikel 8 der Europäischen Menschenrechtskonvention. Es hat also niemand das Recht Informationen zum Privat- oder Familienleben eines anderen ohne dessen Einverständnis zu enthüllen.

## Downloads: nicht alles ist erlaubt...

Installiere legale Software und nutze legale Dienste (Musik, Filme, ...)

Als Luxemburger Student ist der Zugriff auf viele Ressourcen (Office 365 für Bildung, EduCloud, ...) für dich kostenfrei oder vergünstigt (non-profit, „Bildungstarife“).



**bee-secure.lu/legal**

Nutze keine Download-Plattformen (Peer-to-Peer oder direkt) auf illegale Weise.

Illegale Downloads sind nicht nur strafbar, die Plattformen sind auch dafür bekannt eine hohe Anzahl an infizierten Dateien zu enthalten (Viren, Trojaner).

Es gibt mittlerweile eine Vielzahl an legalen Streaming-Möglichkeiten. Einige finanzieren sich über Werbungen und sind daher gratis, andere sind gebührenpflichtig (und verzichten oft auf Werbung).

## 6) Tablets und Smartphones

Tablets und Smartphones sind Rechner (fast) wie die „Großen“. Ihre kleine Größe und ihr mobiler Einsatz bergen jedoch zusätzliche Risiken... so kannst du die Risiken minimieren:

- Sichere das Gerät. Verwende ein starkes Passwort um das Smartphone oder das Tablet zu sperren. Gib dich nicht mit einem 4-Zahlen-PIN zufrieden! Falls das Gerät gestohlen wird, gewinnst du Zeit, um die Daten auf deinem Smartphone oder Tablet auf Distanz zu löschen indem du dich auf dein Konto einloggst.
- Denk nach, bevor du eine App installierst. Überprüfe auf welche Daten die App Zugriff haben wird, bevor du sie installierst. Manche Apps haben zum Beispiel Zugriff auf die Ortung, deine Kontakte, dein Profil bei sozialen Netzwerken... Installiere nur Apps, die du wirklich brauchst und die du auf vertrauenswürdige Quellen zurückführen kannst.
- Bleib vorsichtig mit WiFi Hotspots. Vermeide es persönliche Daten anzugeben oder dich einzuloggen, wenn du einen öffentlichen oder ungesicherten Zugang nutzt.
- Deaktiviere WiFi, Bluetooth, NFC und ähnliche Funktionen, wenn du sie nicht nutzt.
- Das kleine Plus: richte einen zusätzlichen Code für den Zugriff auf die Einstellungen des Tablets oder des Smartphones ein. So vermeidest du, dass ein „Freund“ deine Einstellungen ohne dein Wissen ändert.
- Wenn du das Tablet mit anderen teilst, erstelle unterschiedliche Konten für jeden Benutzer.

Um mehr über die Risiken in Verbindung mit Smartphones zu erfahren:



[bee-secure.lu/phon](http://bee-secure.lu/phon)

## 7) Die Cloud



Mithilfe der Cloud, kannst du von überall auf deine Dokumente, Fotos, Videos und alle anderen Arten von Dateien zugreifen, egal von welchem Rechner oder Terminal. Auf diese Art und Weise brauchen wir unsere Dokumente nicht auf unterschiedliche Geräte zu kopieren, um auf sie zugreifen zu können. Die Cloud erleichtert die Fernarbeit und ermöglicht es mehreren Leuten gleichzeitig an einem Dokument zu arbeiten, ohne dabei am selben Ort zu sein.

Die Cloud macht unsere Arbeit effizienter und hilft uns Dokumente zu speichern. Aber sie birgt auch Risiken. Um diese Risiken einzuschränken, gelten ein paar grundsätzliche Regeln:

1. Verwende ein starkes Passwort um dich in Deine Cloud einzuloggen (*siehe § Passwort Seite 7*).
2. Nutze die doppelte Authentifizierung wenn immer dies möglich ist.
3. Verschlüssele deine Dokumente und sensiblen Daten, die in der Cloud gespeichert sind (*siehe §1, „Verschlüsselung von Daten“ Seite 3*).
4. Schütze alle Geräte, die Zugang zu deiner Cloud haben (*siehe § Tablets und Smartphones Seite 15*).

Lies dir die Nutzungsbedingungen und Garantien der verschiedenen Cloud-Anbieter genau durch. Hier einige Fragen, die es zu überprüfen gilt:

- ☐ Wer hat Zugriff auf deine Daten?
- ☐ Was darf der Cloud-Anbieter mit deinen Daten machen?
- ☐ Welche Datenschutzgarantien werden angeboten?
- ☐ Was passiert bei einer Unterbrechung oder bei der Einstellung der Dienstleistung?
- ☐ Werden deine Daten wirklich zerstört wenn du sie löschst?



[bee-secure.lu/cloud](https://bee-secure.lu/cloud)