

# Internet survival guide



**BEE**  
**SECURE**

Tipps für mehr Sicherheit im Netz

 **CASES**  
SECURITY MADE IN LETZEBUERG

**Dieser Leitfaden soll Studierenden helfen, ihren persönlichen Rechner sowie ihre Daten in einer unbekannt und daher möglicherweise feindseligen Umgebung zu schützen. Ein Rechner ist leicht ersetzbar, eine verloren gegangene Studienarbeit dagegen nur schwer.**

Viele Studenten leben in Wohnheimen oder Wohngemeinschaften und teilen daher ihren Internetzugang, ihr lokales Netzwerk oder ihren Router mit anderen Benutzern. Auch der Internetzugriff an der Universität oder über öffentlich zugängliche Netze (z.B. Hotspots oder Internetcafés) birgt gewisse Risiken.

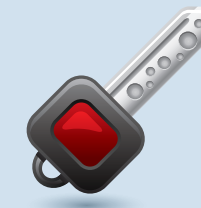


## 1) Die physische Sicherheit

- Verschießen Sie die Tür Ihres Zimmers, um Diebstählen vorzubeugen. Laptops, die an öffentlichen Orten benutzt werden, sollten mit einem Antidiebstahl-Kabel gesichert werden.
- Bewahren Sie Sicherheitskopien ihrer Daten so auf, dass diese nicht direkt zugänglich sind. Verschlüsseln Sie wenn möglich Ihre Festplatten sowie ihre Backups.
- Sperren Sie den Zugriff auf das BIOS mit einem Passwort und beschränken Sie die Boot-Möglichkeiten auf die Festplatte.

### Daten verschlüsseln :

Alle modernen Betriebssysteme bieten die Möglichkeit, Daten auf der Festplatte zu verschlüsseln: „Bitlocker“ unter Microsoft Windows oder „FileVault“ unter Apple OS X. Als kostenloses Tool, das unter allen Betriebssystemen läuft, bietet sich „TrueCrypt“ an:  
<http://tools.cases.lu/CBW>



## 2) Die Konfiguration des Systems

- **Benutzerkonten:** verwenden Sie nicht ständig ein Konto mit Administrator-Rechten. Verwenden Sie unterschiedliche, «eingeschränkte» Benutzerkonten, welche alle Passwortgeschützt sind, um im Internet zu surfen, zu spielen oder zu arbeiten. Aktivieren Sie bei Bildschirmschonern oder dem Stromspar-Modus die Passwortabfrage.
- **Das Passwort:** Verwenden Sie Passwörter mit einer Mindestlänge von 8 Zeichen, bestehend aus Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen. Ein gutes Passwort sollte nicht in einem Wörterbuch enthalten sein und nicht auf persönlichen Daten (Name, Geburtsdatum, etc.) basieren. Ersetzen Sie stets die Standard-Passwörter und ändern Sie regelmäßig Ihre verschiedene Passwörter, am Besten eines pro Konto oder Online-Dienst. Teilen Sie niemandem ihre Passwörter mit.

### Wahl eines Passworts:

Suchen Sie sich einen einprägsamen Satz aus, beispielsweise „Ziehen sie voll Mörderdrang Niep und Piep die Haelse lang!“ (Wilhelm Busch). Nimmt man von jedem Wort den Ersten Buchstaben, so erhält man: „ZsvM-NPdH!““. Durch das Ersetzen einiger Zeichen mit Ziffern entsteht anschließend: „**ZsvMNuPdH1!**““.



- **Updates:** Aktivieren Sie die automatische Update-Funktion ihres Betriebssystems und aller Anwendungen. Falls diese Funktion fehlt, überprüfen Sie regelmäßig die Webseiten der Anbieter auf neue Versionen.

- **Antivirenprogramm:** Installieren Sie ein Antivirenprogramm, das automatisch upgedatet wird. Kostenlose Lösungen finden Sie hier: <http://tools.cases.lu/jTb>. Scannen Sie regelmäßig Ihren Computer nach Malware. Verlassen Sie sich nur auf Warnungen Ihres eigenen Antiviren-Programms und ignorieren Sie Warnungen die Sie via Internet oder Email erhalten.

- **Firewall:** Aktivieren Sie die Firewall Ihres Rechners. Alle modernen Betriebssysteme bieten einen solchen Schutz. Kostenlose Lösungen sind ebenfalls verfügbar.

- **Sicherheitskopien:** Verwenden Sie die Backup-Funktionen ihres Betriebssystems. Speichern Sie Ihre Sicherheitskopien möglichst verschlüsselt auf externen Festplatten.

- **Web-Browser:** Benutzen Sie einen automatisch aktualisierten Browser. Vermeiden Sie unnötige Erweiterungen (Plugins oder Toolbars). Die Verwendung folgender Erweiterungen wird allerdings dringend empfohlen:

- **WOT (Web of Trust)** eine Erweiterung, die Sie vor Websites mit zweifelhaftem Ruf warnt: <http://tools.cases.lu/837>

- **Noscript:** verhindert das Ausführen potenziell bösartiger Skripte: <http://tools.cases.lu/Fh8>

- **https everywhere:** Die Kommunikation mit dem Server erfolgt falls möglich immer verschlüsselt (nur unter Firefox): <http://tools.cases.lu/o80>

- **Flashblock:** Inhalte für Adobe Flash, welche häufig Angriffsflächen bieten, werden unterbunden (nur unter Firefox, Chrome und anderen Browsern): <http://tools.cases.lu/03g>

- **Drahtlose Netzwerke (WiFi):** Sichern Sie Ihren drahtlosen Zugangspunkt (WiFi-Router) mittels WPA2-Verschlüsselung und ändern Sie regelmäßig das Passwort.

- **Bluetooth Netzwerk:** Bei Nichtgebrauch ausschalten.

- **Datenaustausch:** Deaktivieren Sie die gemeinsamen Nutzung von Daten und Ressourcen (Internetzugang, Festplatten, Drucker, usw.), sobald diese nicht mehr benötigt wird.

## 3) Verhaltensregeln

### Seien Sie wachsam!

Seien Sie misstrauisch und hüten Sie sich vor Betrug im Internet. Ihr Verhalten hat direkte Auswirkungen auf die Sicherheit ihrer Daten.

#### • Die Navigation im Internet:

- Vermeiden Sie es unter allen Umständen, auf fremden Rechnern Einkäufe oder Bankgeschäfte zu tätigen.
- Wenn Sie ein Passwort eingeben müssen, verwenden Sie die «Private Browsing»-Funktion (Strg-Shift-P unter Firefox oder Internet Explorer) - Weder ihr Passwort noch andere personenbezogenen Daten werden dann gespeichert.
- Falls Ihr Browser eine Warnung anzeigt, dass das Zertifikat einer SSL-gesicherten Seite (mit dem Präfix https) ungültig ist, verlassen Sie die Webseite ohne irgendwelche Transaktionen zu tätigen.

#### • E-Mails:

- Beantworten Sie niemals E-Mails, die vertraulichen Informationen erfragen (z.B. Passwörter, Kontonummern, Kreditkartendaten).
- Öffnen Sie niemals Links oder Anhänge von E-Mails, falls Sie deren Herkunft nicht mit absoluter Gewissheit kennen.
- Prüfen Sie jede eingehende Mail kritisch bevor Sie handeln.
- Bedenken Sie immer, dass eine E-Mail-Adresse leicht gefälscht werden kann.

#### • Spam:

- Nutzen Sie zwei E-Mail Adressen eine Hauptadresse für vertrauenswürdige Empfänger, sowie eine zweite Adresse (oder eine Alias-Adresse) für öffentliche Kontakte.
- Teilen Sie Ihre Mailadresse nicht Jedermann mit und vermeiden Sie es, diese sie an öffentlichen Stellen preis zu geben (z.B Facebook, Blogs, schwarzes Brett, usw.)

- Antworten Sie unter keinen Umständen auf Spam.
- Nutzen Sie automatische «out of office»-Antworten mit Vorsicht.

#### Hoaxes:

- Vermeiden Sie es, Hoaxes, Falschmeldungen oder Fehlinformationen weiterzuleiten:
- Vor Computerviren wird nie offiziell per E-Mail gewarnt.
- Sicherheits-Updates werden nie via E-Mail verschickt.
- Vorsicht bei Kettenbriefen.
- Überprüfen Sie Informationen mit Hilfe von sicheren Quellen: <http://tools.cases.lu/03M>

#### Soziale Netzwerke und Datenschutz:

- Beschränken Sie die Verbreitung personenbezogener Informationen im Netz weitest möglich.
- Vermeiden Sie es, private Fotos auf sozialen Netzwerken (Facebook, Flickr, Twitter, Studi VZ, usw.) zu veröffentlichen.



## 4) Rechtliche Aspekte

### Handeln Sie verantwortungsvoll!

Sie sind nicht anonym im Netz. Sie müssen die Gesetzgebung jener Länder befolgen, in denen Sie online sind.

- Der Abonnent einer Internetanbindung ist für die Verwendung dieser Anbindung verantwortlich. Derzeit wird eine Harmonisierung des europäischen Rechtsrahmens gegen Internetkriminalität angestrebt. Ziel ist auch der Schutz des Urheberrechts. Die Frage nach der Verantwortung beschränkt sich nicht auf die Straftat, sondern darauf, wem der Internetzugang gehört, der zur Ausführung genutzt wurde.
- Zum Thema illegale Downloads: die meisten europäischen Länder ahnden Vergehen gegen das Urheberrecht: <http://tools.cases.lu/H2q>. Nutzen Sie keine Download-Plattformen (z.B. Peer-to-Peer, Bittorrent) auf illegale Weise, da die Folgen schwerwiegend sein könnten (sie reichen von Geldstrafen bis zum Kappen der Internetverbindung).
- Seien Sie vorsichtig beim Verfassen von Texten und Kommentaren oder beim Veröffentlichen von Fotos oder Videos im Netz – Die bestehenden Gesetze zur Diffamierung und zum Schutz der Privatsphäre sind anwendbar.

