

Security-Tipps

Sicherheitstyps für die Anwendung der Informationstechnologie (IT)
von deutschen Bundesamt für IT-Sicherheit

Security-Tipps

Fünf Grundregeln

1. Updates

Firmware und Software auf dem neusten Stand halten
(Betriebssystem und alle Programme)

2. Passwörter

Starke und unterschiedliche Passwörter verwenden
(Passwortmanager verwenden)

3. 2 Faktor Authentifizierung verwenden

Zweiter Faktor z.B.: Fingerabdruck oder TAN
(TAN = Transaktionsnummer per SMS, Spez. App oder Gerät)

4. Virenschutz

Der im Windows vorhandene Virenschutz genügt.

5. Firewall

Die 'Feuerwand' schützt den PC, dass Programme nicht ohne Weiteres kontakt mit dem Internet aufnehmen können.

Wenn sich die Firewall meldet um eine Ausnahme zu genehmigen ist Vorsicht geboten.

Security-Tipps

Sicher im Internet

- **Browser absichern**

Tor-Browser oder Firefox-Browser verwenden

In den Firefox Einstellungen 'strenger Schutz vor Aktivitätsverfolgung' einstellen,
nur HTTPS-Modus aktivieren

Add-On 'uBlock Origin' installieren.

((Achtung! Der Privat-Modus in den Browsern funktioniert nur lokal am PC.

(Andere PC-Benutzer können die Aktivitäten nicht einsehen)

Gegen aussen (Internet) funktioniert das nicht))

Security-Tipps

Sicher im Internet (Firefox)

Einstellungen – Datenschutz & Sicherheit

Der Browser wird durch Ihre Organisation verwaltet. In Einstellungen suchen

Standard
Ausgewogen zwischen Schutz und Leistung. Seiten laden normal.

Streng
Stärkerer Schutz, einige Websites oder mancher Inhalt funktioniert eventuell nicht.

Firefox blockiert Folgendes:

- Skripte zur Aktivitätenverfolgung durch soziale Netzwerke
- Inhalte zur Aktivitätenverfolgung in allen Fenstern
- Heimliche Digitalwährungsberechner (Krypto-Miner)
- Identifizierer (Fingerprinter)

Achtung!
Diese Einstellung kann dazu führen, dass einige Websites nicht korrekt Inhalte anzeigen oder funktionieren. Wenn eine Website defekt zu sein scheint, können Sie den Schutz vor Aktivitätenverfolgung für diese Website deaktivieren, um alle Inhalte zu laden.
[Weitere Informationen](#)

Nur-HTTPS-Modus
HTTPS bietet eine sichere, verschlüsselte Verbindung zwischen Firefox und den von Ihnen besuchten Websites. Die meisten Websites unterstützen HTTPS und wenn der Nur-HTTPS-Modus aktiviert ist, wird Firefox alle Verbindungen zu HTTPS aufrüsten.
[Weitere Informationen](#)

Nur-HTTPS-Modus in allen Fenstern aktivieren [Ausnahmen verwalten...](#)

Nur-HTTPS-Modus nur in privaten Fenstern aktivieren

Nur-HTTPS-Modus nicht aktivieren

Security-Tipps

Sicher im Internet

- **Augen auf bei E-Mails**

Kenne ich den Absender?

Vorsicht beim Öffnen von Anhängen.

Vorsicht beim Anklicken von Bildern.

Vorsicht beim Anklicken von Links.

- **Vorsicht bei Downloads**

Laden Sie nur Daten von bekannten und seriösen Quellen herunter.

(z.B.: Chip.de)

Security-Tipps

Sicher im Internet

- **Online Dienste (Cloud-Speicher)**

Überlegen Sie, wem Sie persönliche Daten anvertrauen.

Erben sollten auf den Online Dienst zugreifen können (Digitaler Nachlass)

- **Backups machen**

Regelmässig Sicherungskopien anfertigen. (Backup-Programme nutzen)

(Ein Backup ist nur dann nützlich wenn man geübt hat

wie verlorene Daten wieder hergestellt werden können!)

Security-Tipps

WLAN absichern

- Passwort des Routers ändern (Initialpasswort ist bei manchen Router-Modellen bekannt)
- Router Firmware aktuell halten.
- Unnötige Funktionen abschalten (z.B.: Fernzugriff)

Handys absichern

- Apps aktuell halten
- Bildschirmsperre kurz einstellen
- App-Berechtigungen kritisch hinterfragen
(z.B.: Taschenlampen-App benötigt kein Zugriffsrecht auf die Kontakte)

Irrtümer aufgeklärt

- **Irrtum:**
Meine PC-Firewall schützt mich vor allen Angriffen aus dem Internet.
- **Richtig ist:**
Ohne die richtige Konfiguration bietet eine Firewall keinen optimalen Schutz vor Angriffen aus dem Internet.
- So sollten die Einstellungen regelmäßig überprüft und die Filterregeln so definiert werden, dass nur unbedingt notwendige Zugriffe erlaubt sind. Verlangt ein nicht bekanntes Programm Zugriff auf das Internet, sollten Sie dies kritisch prüfen.

Irrtümer aufgeklärt

- **Irrtum:**
Wenn ich einen aktuellen Virensch scanner habe, muss ich Updates für andere Software nicht sofort installieren.
- **Richtig ist:**
Zwar ist ein Virenschutz wichtig für sicheres Surfen im Internet – Updates für die genutzten Anwendungen sollten jedoch immer schnellstmöglich installiert werden.
- Aktuelle Schadsoftware kann bestehende Sicherheitslücken ausnutzen, bevor sie von Virenschannern erkannt wird.

Irrtümer aufgeklärt

- **Irrtum:**
Ein einziges langes Buchstaben und Zeichen-Passwort reicht für meine Online-Dienste vollkommen aus.
- **Richtig ist:**
Nein, denn sollte ein Online- Dienst kompromittiert und Ihr Passwort gestohlen werden, sind alle mit diesem Passwort geschützten Dienste in Gefahr.
- Nutzen Sie deshalb für jeden Zugang ein eigenes, starkes Passwort.

Irrtümer aufgeklärt

- **Irrtum:**
Ich surfe nur auf vertrauenswürdigen Seiten, darum muss ich mich nicht vor Cyber-Angriffen schützen.
- **Richtig ist:**
Leider können auch vertrauenswürdige Seiten hin und wieder von Schadsoftware betroffen sein.
- Werbebanner
- Drive-by-Downloads
- Skripte in populären Internet-Seiten.

Irrtümer aufgeklärt

- **Irrtum:**

Ich habe nichts zu verbergen und keine wichtigen Daten, also bin ich doch kein Ziel für Cyber-Kriminelle und muss mich deshalb nicht schützen.

- **Richtig ist:**

Diese Ansicht ist grundlegend falsch, da Cyber-Kriminelle alle verfügbaren Daten für ihre Zwecke nutzen können.

- Erpressung

- Missbrauch für Spam-Versand oder Krypto-Mining

Danke für Ihre Aufmerksamkeit