



Freistaat
SACHSEN

10 Goldene Regeln

für Informationssicherheit



10 Goldene Regeln

für Informationssicherheit

1. Software auf dem aktuellen Stand halten

Bei Betriebssystemen und Anwendungen werden immer wieder Schwachstellen bekannt, die die Sicherheit Ihres Computers gefährden. Installieren Sie regelmäßig die Aktualisierungen der Hersteller. **Gut für Sie: In Ihrer Behörde erledigt das bereits Ihr IT-Service.**

2. Aktuellen Virens Scanner verwenden

Ein aktueller Virens Scanner gehört zum Basischutz eines jeden Computers. Achten Sie darauf, dass dieser aktiviert ist und auf dem aktuellen Stand gehalten wird. Der Virens Scanner sollte jedoch nicht zur Gedankenlosigkeit verleiten, da er keinen absoluten Schutz bieten kann! **Gut für Sie: In den zentralen Diensten des SVN, in den Behörden und auf Ihrem Arbeitsplatz-PC gibt es einen dreistufigen Virenschutz.**

3. Daten mit einer Firewall schützen

Eine Firewall schützt Ihren Computer vor unberechtigten Zugriffen aus dem Internet bzw. aus dem Netzwerk, in dem Sie arbeiten. Die oft bereits im Betriebssystem enthaltene Firewall sollte deshalb unbedingt dauerhaft aktiviert werden. **Gut für Sie: Auf Ihrem Arbeitsplatz-PC gehen Sie automatisch mit Firewall ins Netz.**

4. Sichere Passwörter verwenden

Sichere Passwörter besitzen eine Mindestlänge von 12 Zeichen und setzen sich aus mindestens drei von vier Zeichenarten (Groß-/Kleinschreibung, Ziffern, Sonderzeichen) zusammen. Zur Passwortgenerierung können individuelle Merksätze oder Tools wie bspw. Passwortkarten genutzt werden. **Persönliche Bezüge wie Haustiernamen, Hobbys in Passwörtern oder im Privaten genutzte Passwörter sollten dabei vermieden werden.**

8. Informationssicherheit betrifft nicht nur den Computer

Wenn Sie Ihr Büro verlassen - und sei es nur für eine kurze Kaffeepause - sichern Sie Ihr Büro vor unbefugtem Zugriff, indem Sie die Tür verschließen. **Sensible Informationen sind auch auf Papier ein lohnenswertes Objekt für Datendiebe.**

9. Nie aus Drucksituationen heraus handeln

Werden Sie hellhörig, wenn Sie um die Herausgabe von persönlichen Informationen von Ihnen oder von Dritten gebeten werden – egal ob Passwort, Telefonnummer oder Informationen aus dem Terminkalender. Gleiches gilt, wenn unerwartet per E-Mail oder Telefon von angeblich „höchster Stelle“ geheim zu haltende Handlungen angeordnet werden. **Handeln Sie nie aus einer Drucksituation heraus! Atmen Sie durch und gehen Sie der Sache mit einem Kollegen auf den Grund.**

10. Informationen nicht leichtfertig preisgeben

Vom zu lauten Gespräch über Dienstliches in der Straßenbahn bis hin zu Einträgen in sozialen Netzwerken mit vertraulichen Informationen Ihrer Behörde oder Hinweisen zu Ihrem Passwort: **Tragen Sie Sorge dafür, dass Dienstliches auch dienstlich bleibt.**



5. Nicht mit Administratorrechten arbeiten

Wenn Sie mit Administratorrechten auf Ihrem Computer arbeiten, haben auch Schadprogramme uneingeschränkten Zugriff auf Ihr System und können so ihre volle Wirkung entfalten. Arbeiten Sie im Alltag deshalb unter einem Benutzer-Konto mit eingeschränkten Rechten. **Gut für Sie:** Auf Ihrem Arbeitsplatzrechner sind die Zugriffsrechte automatisch eingeschränkt.

6. Vorsicht bei E-Mail-Anhängen und Links

Um den Eintritt schädlicher Software zu vermeiden, sollten Sie nie leichtfertig Anhänge und Links in E-Mails von Absendern öffnen, von welchen Sie keine Mail erwarten. Oft sind böartige E-Mails auch an Rechtschreibfehlern oder am fehlenden dienstlichen Kontext erkennbar. Jeder geöffnete Anhang oder geklickte Link aus einer E-Mail heraus kann die Sicherheit Ihres Computers und des gesamten Netzes gefährden. **Im Zweifel oder bei einem ungewöhnlichen Verhalten des Computers nach der Öffnung verdächtiger E-Mails sollten Sie stets Ihren IT-Service kontaktieren.**

7. Daten regelmäßig sichern

Eine regelmäßige Sicherung mittels „Backup“ Ihrer wichtigen Daten schützt diese vor Verlust. Nur gesichert ist sicher! **Gut für Sie:** In Ihrer Behörde erstellt Ihr IT-Service regelmäßige Backups.



Informationssicherheit

Es kommt auch auf Sie an!

Mehr als Regeln:

Das E-Learning

„Informationssicherheit am Arbeitsplatz“

Wenn Sie mehr zur Informationssicherheit erfahren und wissen wollen, melden Sie sich doch für das E-Learning Angebot zur „Informationssicherheit am Arbeitsplatz“ an.

Bereits über 18.000 Mitarbeiterinnen und Mitarbeiter von Landes- und Kommunalbehörden in Sachsen haben den Online-Kurs belegt und die meisten von ihnen auch den Test zum Sächsischen Informationssicherheitsschein absolviert und bestanden.

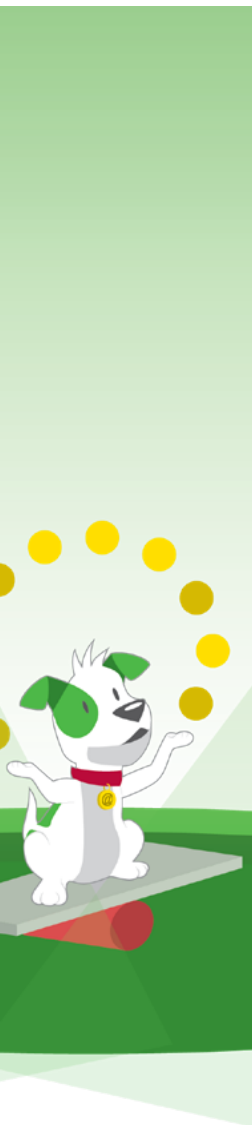
Im E-Learning werden die wichtigsten Themenbereiche anschaulich und prägnant dargestellt. Durch die Gliederung in Bausteine ist eine zeitlich flexible Bearbeitung der einzelnen Themenkomplexe möglich ohne den Verlust des vorherigen Bearbeitungsstandes.

Ziel dieses Angebots ist es, Sie über Passwortsicherheit, Phishing-Angriffe, Datendiebstahl etc. zu informieren und Ihnen den Blick für Schwachstellen im Arbeitsumfeld zu weiten.

Melden Sie sich kostenfrei an unter:

<https://web1.extranet.sachsen.de/Lernwelt>



**Herausgeber:**

Sächsische Staatskanzlei
Archivstraße 1
01097 Dresden

Redaktion:

Referat 45
Informations- und Cybersicherheit,
Kritische Infrastrukturen

Gestaltung und Satz:

Torux - Kreativleistung nach Maß, Dresden

Druck:

Wir machen Druck

Redaktionsschluss:

Mai 2022

Bezug:

Die Broschüre steht auch barrierefrei zum
Download zur Verfügung.

www.publikationen.sachsen.de

