Informatik und Dienstleistungen

OCOM Ratgeber zum Tag der Computersicherheit: Goldene Regeln zu Passwörtern, Backup- Antiviren-Lösungen und sicheres Arbeiten am PC.

Der Tag der Computersicherheit findet jährlich am 30. November statt. Der Aktionstag wurde im Jahr 1988 in den USA von der Vereinigung für Computersicherheit ins Leben gerufen. Er soll die Menschen erinnern, ihre Computer und ihre persönlichen Daten abzusichern. An diesem Tag wird es höchste Zeit wieder einmal ein Backup zu erstellen, sämtliche Software upzudaten, die Antivieren-Software zu kontrollieren und seine Passwörter zu ändern.

1. Sichere Passwörter

Noch immer werden viel zu oft zu simple Passwörter wie «123456» oder «Passwort» verwendet.
Wir zeigen Ihnen, wie Sie ganz einfach schwer zu erratende Passwörter kreieren, die Sie sich auch merken können.

Einfache Chiffriermethoden für bestehende und neue Passwörter

Falls Sie sich von Ihren bisherigen Passwörtern nicht trennen möchten, können diese schon mit wenigen Handgriffen sicherer gemacht werden:

- Buchstaben im Alphabet verschieben
  Mit dieser Methode werden die einzelnen Buchstaben des Passwortes in der Reinfolge des Alphabets nach oben oder unten verschoben. Wenn z.B. Ihr Passwort «MeinComputer#1» lautet, wäre das dann nach dem Verschieben nach oben «NfjoDpnqvufs#1» oder «LdhmBnlotsdq#1» bei der Verschiebung nach unten.

- Buchstaben auf der Tastatur verschieben
  Grundsätzlich der gleiche Ansatz wie im Punkt 2, nur ersetzt man hier die Buchstaben im Passwort mit jenem Schriftzeichen, das auf der Tastatur benachbart ist. Also aus unserem «MeinComputer#1» wird nun «,romVp,üzrt#1).

Ein neues sicheres Passwort erstellen

- Passwort aus einem Satz
  Eine ganz einfache und gute Methode um ein sicheres Passwort zu kreieren. Nehmen Sie einen Satz, den Sie sich gut merken können, und bilden Sie Ihr Passwort aus den jeweiligen Anfangsbuchstaben und Ziffern:

  «Meine Mutter Ursula hat am 12.Januar Geburtstag! »

  So entsteht ein Passwort aus einer beliebigen Zeichenfolge, dass Sie sich gut merken können.

  «MMUha12.JG!»

Kombiniert man dies mit einer der oben bereits erwähnten Chiffriermethoden, wird das Passwort noch sicherer.

OCOM AG Informatik und Dienstleistungen
Englisch-Gruss-Strasse 6, Postfach 556, 3902 Brig-Glis
OCOM STORE Kantonsstrasse 21, 3902 Brig-Glis
T 027 922 10 10, F 027 922 10 11, ocom@ocom.ch, www.ocom.ch

Passwörter mit zeitlicher Beschränkung kreieren

Immer öfter müssen für bestimmte Dienste in bestimmten Zeitabständen die Passwörter geändert werden.
Hier hilft das Passwort mit dem «Gültigkeitszeitraum» zu erweitern.
So kann man ganz einfach z.B. jeden Monat ein neues Passwort erstellen.
Aus «MMUha12.JG!» aus dem vorgehenden Beispiel wird dann einfach «MMUha12.JG!01.18».

8 Regeln zum Sicheren Passwort – Verwenden Sie:

- mindestens 10 Zeichen
- Keine Wörter die man im Duden oder anderen Wörterbüchern finden kann
- immer eine Mischung aus Klein- und Grossbuchstaben, Zahlen und Sonderzeichen
- keine Reihenfolgen verwenden wie «asdfgh» oder «123456»
- keine benutzerbezogenen Daten in Ihrem Passwort.
- ändern Sie Ihre Passwörter von Zeit zu Zeit
- auf keinen Fall für alle Zugänge dasselbe Passwort
- speichern Sie Ihr Passwort nie unverschlüsselt ab

Passwort-Sicherheit überprüfen

Unter «https://review.datenschutz.ch/passwortcheck/check.php» können Sie die Sicherheit Ihres Passwortes überprüfen. Nehmen Sie dazu nicht Ihr echtes Passwort, sondern ein ähnliches.

2. Regelmässige Datensicherung

Die Datensicherung gehört immer noch zu den vernachlässigten Themen im EDV-Bereich.
Ob im Geschäft oder Zuhause - die meisten Benutzer gehen mit ihren Daten viel zu sorglos um. Auch wenn das Problem "Internetkriminalität" inzwischen viele Benutzer sensibilisiert hat und die meisten PCs gegen Angriffe von aussen gut gesichert sind, machen sich immer noch zu wenig Anwender Gedanken, wie Sie Ihre Daten vor Verlust schützen können.

Ein Datenverlust entsteht nicht nur durch Hackerangriffe. So kann es schnell passieren, dass durch einen Benutzerfehler die gespeicherten Daten unwiederbringlich verloren gehen. Auch durch Hardwarefehler, einen Festplattencrash oder äussere Einwirkungen können Daten verloren gehen. Der Verlust von geschäftsrelevanten wie auch privaten Daten kann verhängnisvolle Folgen haben. Dabei ist es so einfach, durch regelmässige Backups alle wichtigen Daten zu sichern. Das Problem liegt daher auch nicht in der Komplexität der Handhabung, sondern in der Sorglosigkeit der meisten Anwender.

7 Tipps für eine effektive Datensicherung

1. Daten regelmässig sichern
   Die Sicherungsintervalle sind abhängig davon, wie oft die zu sichernden Daten bearbeitet bzw. aktualisiert werden. Je häufiger die Bearbeitung der Daten, desto kürzer die Sicherungsintervalle.

2. Auf externen Speichermedien sichern und getrennt aufbewahren
   Die Daten sind auf externen Speichermedien zu sichern. Also nicht auf einer eigenen Partition auf der Festplatte, sondern ausserhalb des Computers. Das Backup sollte zudem ausser Haus gelagert werden (Schutz vor Elementarschäden).

3. **Backup testen**
   Die ganze Datensicherung bringt nichts, wenn die Daten bei Verlust nicht wiederhergestellt werden können. Deshalb sollten Sie stets testen, ob die Rücksicherung problemlos funktioniert.

4. **Welche Daten sichern**
   Überlegen Sie genau, welche Daten Sie regelmässig sichern wollen. So ist es z.B. oftmals nicht sinnvoll, Programmdateien immer mit zu sichern, da diese durch eine Neuinstallation problemlos wiederhergestellt werden können.

5. **Achtung bei Neuinstallationen**
   Vor allem vor Neuinstallationen von Programmen sollten Sie eine Datensicherung durchführen. Es kann durchaus vorkommen, dass nach der Installation eines Programms nicht mehr alles so funktioniert, wie es funktionieren sollte.

6. **Eindeutige Bezeichnung**
   Aus dem Backup sollte genau hervorgehen, welche Dateien mit welchem Stand sich auf dem Sicherungsmedium befinden.

7. **Mehrere Backup-Medien verwenden**
   Auch ein Backup kann aus den oben genannten Gründen ausfallen. Aus diesem Grund ist es empfehlenswert, dass Sie Kopien Ihrer Daten auf mindestens zwei unterschiedlichen Speichertypen aufbewahren sollten, beispielsweise auf zwei externen Festplatten.

Füllen Sie das Formular unter https://www.ocom.ch/dienstleistungen/loesungen aus und wir unterbreiten Ihnen unverbindlich Ihr individuelles Backup-Angebot.

3. Antivieren-Lösung

Wer heutzutage im Internet unterwegs ist, kommt um einen guten Virenscanner nicht mehr herum. Täglich drohen neue Gefahren in Form von Viren, Trojanern und sonstiger Schadsoftware. Wie schütz man sich am besten und wo liegt der Unterschied zwischen einer gratis Antivirensoftware und einer gekauften?

Grundsätzlich liegt der Unterschied einer Gratisversion zu einer Bezahlversion in erster Linie an der Erkennung von Viren. Hier werden zwei Techniken unterschieden:

Bei Gratissoftware kommt die sogenannte **reaktive Erkennung** zum Einsatz.
Bei dieser Art der Erkennung wird ein Schädling erst erkannt, wenn eine entsprechende Signatur seitens des Herstellers der Antivirensoftware zur Verfügung gestellt wurde. Nachteil hierbei: Ohne aktualisierte Signaturen werden keine neuen Schadprogramme erkannt. Ein markanter Nachteil einer Gratisversion ist auch, dass diese meist mit Werbung und Benachrichtigungen versehen sind. Meist steht hinter einer freien Version auch eine bezahlte Version desselben Herstellers und die wird natürlich angepriesen.

Beim von uns empfohlenen OCOM Managed Antivirus wie auch in andern Kaufversionen wird eine **proaktive Erkennung** eingesetzt:
Diese bezeichnet die Erkennung von Viren, ohne dass eine entsprechende Signatur zur Verfügung steht. Beim Proaktiven Verfahren wird nach allgemeinen Merkmalen und Verhaltensweisen von Viren gesucht, um unbekannte Schadprogramme zu erkennen. Die Wichtigkeit dieser – präventiven – Art der Erkennung nimmt stetig zu, da die Zeiträume in denen neue Viren und Varianten eines Virus in Umlauf gebracht werden, immer kürzer werden. Für die Antivirenhersteller wird es somit immer aufwendiger und schwieriger, alle Schädlinge zeitnah durch eine entsprechende Signatur zu erkennen.

Die aktuellen Tests untermauern den Unterschied der Kauf und gratis Versionen: Auf den ersten 10 Plätzen stehen ausnahmslos die Kaufversionen.

Egal welches Antivirus, das Wichtigste ist immer: Benutzen Sie ein aktuelles Virenschutzprogramm und halten Sie es auf dem aktuellen Stand.

Bei Fragen zu Antivieren-Lösungen können Sie sich gerne bei uns melden.

4. Allgemeine Tipps für ein sicheres Arbeiten am PC

1. Den PC-Arbeitsplatz im Büro und Zuhause in Sachen Sicherheit überprüfen. Sind die Kabel richtig verlegt, gibt es Steckdosen oder Kabel mit Wackelkontakten oder Störungen?

2. Sind die Geräte am Arbeitsplatz sicher?
   Kann das Büro verlassen werden, ohne das andere Personen Zugang haben oder diese entwenden können? Gerade mobile Geräte wie Tablets oder Notebooks sollten mit entsprechenden Sicherheitsmassnahmen versehen werden.

3. Aufgepasst bei E-Mails:
   Hacker verstecken Ihre Schadsoftware meist in E-Mail-Anhängen oder hinter Links, die auf möglichst interessante Webseiten führen sollen. Da hilft nur: Öffnen Sie keine ungefragt erhaltenen Mailanhänge - schon gar nicht von unbekannten Quellen - und folgen Sie nicht blind jedem Link.

4. Dubiose Suchergebnisse:
   Seien Sie gegenüber fremden und allzu stark angepriesenen Gratisinhalten misstrauisch. Downloads wie Software oder Dateien, nur aus vertrauenswürdiger Quellen machen.

5. Öffentliche WLAN Hotspots:
   WLAN-Hotspots an öffentlichen Plätzen sind nützlich. Doch ein WLAN mit anderen zu teilen bedeutet, dass alle anderen Computer im selben Netz theoretisch mitlesen können: Suchanfragen, Passwörter, Anmeldedaten … In öffentlichen Netzen sollte man Websites nur über https:// aufrufen.

6. Hacker dringen regelmässig in ungenügend gesicherte Kundendatenbanken ein und stehlen Zugangsdaten wie Email-Adressen und zugehörige Passwörter. Verwenden Sie für jede Website und jeden Dienst unbedingt ein eigenes Passwort. So vermeiden Sie, dass gestohlene Passwörter gleich bei verschiedenen Diensten missbraucht werden können. Wie Sie ein sicheres Passwort erstellen, sehen Sie unter Punkt 1 dieses Ratgebers.

7. Erpresserviren (sog. Ransomware) klauen Ihre Daten und erpressen Sie dann. So verschlüsselt manche Schadsoftware wichtige Dokumente auf Ihrem Computer. Anschliessend wird “Lösegeld” für die Entschlüsselung verlangt. Zahlen Sie niemals ein solches Lösegeld. Sie bekommen Ihre Daten meist nicht zurück. Achten Sie immer darauf, regelmässige Backups ihrer Daten zu erstellen. Mehr zu Backups unter Punkt 2 dieses Ratgebers.

8. Auch ein Computer braucht Pflege.
   Schmutzige Tastatur, Staub auf dem Monitor und anderen Geräten? Die Maus versteckt sich unter einem Stapel von Papier und Kaffeetassen? Auch dieses Chaos sollte am Tag der Computersicherheit mal wieder in Angriff genommen werden.

5. Zusammenfassung

Der Computer und allen voran das Internet ist zu einem bedeutenden Bestandteil unseres Alltags geworden. Im Internet rufen wir Nachrichten ab, chatten und bezahlen Rechnungen. Neben all diesen Möglichkeiten birgt das Internet aber auch sehr viele Gefahren. Unzählige Computerschädlinge versuchen ständig einen Weg in unseren PC zu finden, auf welchem persönliche Daten wie Fotos, Briefe oder wichtige Dokumente gespeichert sind. Bei einem erfolgreichen Angriff können Viren und Trojaner grossen Schaden anrichten, indem sie diese Daten verändern, löschen oder die darin enthaltenen Informationen dazu verwenden, um beispielsweise in Ihrem Namen oder auf Ihre Kosten im Internet einzukaufen.

Einen 100%-Schutz gibt es nicht und wird es nie geben! Das Risiko kann aber vermindert werden, wenn Sie sich an diese einfachen Grundsätze halten:

1. Die Datensicherung ist Ihre Lebensversicherung.
2. Antivirenprogramm installieren und immer aktuell halten.
3. Software auf dem aktuellsten Stand halten.
4. Gesunder Menschenverstand walten lassen. Klicken Sie nicht auf jeden Link, hinterfragen Sie den Inhalt der empfangenen Email und behalten Sie Ihre persönlichen Daten für sich.
5. Schützen Sie auch Ihre Kinder am Computer. Lesen Sie dazu mehr in unserem Ratgeber zum Thema Kindersicherheit unter https://www.ocom.ch/data/Ressources/1496836605-Ratgeber-Kindersicherheit.pdf