

In Unternehmen, Behörden und auch im privaten Bereich ist der Computer heute selbstverständlich. Angesichts der vielfältigen Bedrohungen der Informationstechnologie gilt es für alle verstärkt die folgenden Merkmale zu beachten:

Mehr Informationssicherheit für **Privatanwender**

Das 5-Punkte-Programm der InfoSurance.CH

1. **Datensicherung**

Durchführung und Kontrolle der regelmässigen Sicherung aller Daten auf andere Medien (Bänder, Festplatten, DVD, CD, USB-Sticks).

2. **Virenschutz**

Installation und automatisierte, regelmässige Aktualisierung der Virenschutz-Software.

3. **Firewall**

Zuverlässige Sperrung aller nicht zwingend nötigen Verbindungen im Internet, automatische Überwachung der Aktivitäten mit Alarmierung.

4. **Software-Update**

Automatisierte regelmässige Wartung der Software mit den nötigen Software-Updates der Hersteller.

5. **Verhalten**

Verwenden von persönlichen, starken Passwörtern; verantwortungsvoller Umgang mit persönlichen Informationen; gesundes Misstrauen gegenüber Angeboten aus dem Internet.

Mehr Informationssicherheit am **Arbeitsplatz**

1. **Datensicherung**

Speichern Sie möglichst alle Ihre Daten auf dem Server. Ihr LE sichert diese regelmässig und unterstützt Sie im Notfall bei deren Wiederherstellung.

2. **Virenschutz**

Auf Ihrem Arbeitsplatzsystem muss ein Antivirenprogramm installiert und aktiv sein. Dieses wird regelmässig durch ihren LE aktualisiert.

3. **Datenschutz und Informationsschutz**

Bewahren Sie schützenswerte Informationen vor deren Missbrauch. Entsorgen Sie Papier und Datenträger mit sensitivem Inhalt in den dazu vorgesehenen Behältern (Bsp. Schredder, etc.).

4. **Mail**

Löschen Sie Mails von unbekannten Absendern mit seltsam anmutendem Betreff sofort ungeöffnet und leeren Sie anschliessend den Papierkorb.

5. **Verhalten**

Lassen Sie Ihre mobilen Geräte und Datenträger (Laptop, PDA, USB-Stick etc.) nie unbeaufsichtigt. Ein Diebstahl ist umgehend der zuständigen Stelle zu melden.

Weitergehende Informationen finden Sie auf dem Intranet unter: <http://www.isb.admin.ch/sicherheit>

Que ce soit au sein des entreprises, des autorités ou dans la sphère privée, l'ordinateur fait à présent partie intégrante de la vie de tout un chacun. Vu les nombreux dangers liés aux technologies de l'information, il convient d'observer très attentivement les points suivants:

Une plus grande sécurité de l'information pour les **utilisateurs privés**

Le programme en cinq points d'InfoSurance.ch:

1. Sauvegarde des données

Sauvegarde régulière de toutes les données sur divers supports (bandes, disques durs, DVD, CD, clés USB) et contrôle de la sauvegarde.

2. Protection antivirus

Installation et actualisation automatique et régulière des logiciels antivirus.

3. Pare-feu

Blocage fiable de toutes les connexions Internet qui ne sont pas indispensables, surveillance automatique des activités déclenchant une alarme.

4. Mise à jour des logiciels

Maintenance automatique et régulière des logiciels au moyen des mises à jour appropriées des fabricants.

5. Comportement à adopter

Utilisation de mots de passe personnels et difficiles à deviner; attitude responsable vis-à-vis des informations personnelles; prudence vis-à-vis d'offres Internet.

Une plus grande sécurité de l'information sur le **lieu de travail**

1. Sauvegarde des données

Sauvegardez si possible toutes vos données sur le serveur. Votre fournisseur de prestations (FP) les sauvegardera régulièrement et vous aidera à les récupérer en cas de problème.

2. Protection antivirus

Un antivirus doit être installé et activé sur votre poste de travail. Ce dernier est régulièrement mis à jour par votre FP.

3. Protection des données et des informations

Veillez à protéger vos informations sensibles d'un usage abusif. Détruisez vos documents papier et supports de données sensibles au moyen des machines prévues à cet effet (p. ex. broyeur, etc.).

4. Courriel

N'ouvrez pas les courriels dont vous ne connaissez pas l'expéditeur et dont l'objet vous semble curieux, mais effacez-les immédiatement et videz ensuite la corbeille.

5. Comportement à adopter

Ne laissez jamais vos appareils et supports de données mobiles (ordinateur portable, assistant personnel numérique, clés USB, etc.) sans surveillance. Tout vol doit être immédiatement signalé au service compétent.

Vous trouverez de plus amples informations sur Intranet à l'adresse suivante:
<http://www.isb.admin.ch/sicherheit>.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Al giorno d'oggi il computer fa parte della vita quotidiana di imprese, autorità e privati. In considerazione delle innumerevoli minacce della tecnologia dell'informazione è necessario che tutti osservino scrupolosamente i seguenti punti:

Maggiore protezione delle informazioni per gli **utenti privati**

Il programma di InfoSurance.CH in 5 punti

1. Sicurezza dei dati

Impiego e controllo regolare della sicurezza di tutti i dati su altri mezzi d'informazione (nastri, dischi fissi, DVD, CD e stick USB).

2. Protezione dai virus

Installazione e aggiornamento automatico e regolare del software di protezione dai virus.

3. Firewall

Blocco affidabile di tutti i collegamenti a internet non assolutamente necessari, sorveglianza automatica delle attività con allarme.

4. Software-Update

Manutenzione automatica e regolare del software con i necessari aggiornamenti da parte del produttore.

5. Comportamento

Utilizzo di password personali e sicure; impiego responsabile delle informazioni personali; sana diffidenza verso offerte provenienti da internet.

Maggiore protezione delle informazioni sul **posto di lavoro**

1. Sicurezza dei dati

Salvate il più possibile tutti i vostri dati sul server. Il vostro fornitore di prestazioni li assicura regolarmente e in caso di emergenza vi sostiene nel loro recupero.

2. Protezione dai virus

Nel sistema del vostro posto di lavoro deve essere installato e attivato un programma antivirus. Esso viene regolarmente aggiornato tramite il vostro fornitore di prestazioni.

3. Protezione dei dati e protezione delle informazioni

Protegete dagli abusi le informazioni degne di tutela. Smaltite la carta e i supporti di dati dal contenuto delicato negli appositi contenitori (ad es. sfilacciatrice ecc.).

4. Mail

Cancellate immediatamente le mail di mittenti sconosciuti con oggetto insolito senza aprirle e infine svuotate il cestino.

5. Comportamento

Non lasciate mai incustoditi i vostri strumenti e i supporti di dati mobili (laptop, PDA, stick USB ecc.). Un eventuale furto deve essere immediatamente denunciato all'autorità competente.

Ulteriori informazioni sono disponibili in intranet all'indirizzo:

<http://www.isb.admin.ch/sicherheit>

The computer is a commodity in professional and private life today. In the light of the threats related to information technology, the following points are increasingly important and must be considered:

More information security for **private users**

The 5 point programme of InfoSurance.CH

1. **Data backups**

Carrying out and inspection of regular backups of all data onto other media (tapes, hard disks, DVD, CD and USB sticks).

2. **Virus protection**

Installation and regular, automatic update of virus protection software.

3. **Firewalls**

Reliable access blocking for all internet connections which are not absolutely necessary, automatic monitoring of activities with alerting.

4. **Software updates**

Regular, automatic software maintenance using software updates from the manufacturer.

5. **Behavioural patterns**

Use of personal, strong passwords; handling personal information responsibly; a healthy mistrust of offers via the Internet.

More information security in the **workplace**

1. **Data backups**

As far as possible, store all your data on the server. Your service provider backs up your data regularly and provides support with data retrieval.

2. **Virus protection**

An antivirus programme must be installed and activated on your workstation. It will be updated regularly by your service provider.

3. **Data protection and information protection**

Prevent misuse of information worth protecting. Dispose of paper and data carriers holding sensitive information in the containers provided (e.g. shredders, etc.).

4. **E-mails**

Delete e-mails from unknown sources with suspicious headings and finally empty the Recycle Bin.

5. **Behavioural patterns**

Never leave your mobile appliances and data carriers unattended (laptop, PDA, USB stick, etc.). Thefts should be reported immediately to the competent body.

Further information can be found on the Intranet at

<http://www.isb.admin.ch/sicherheit>