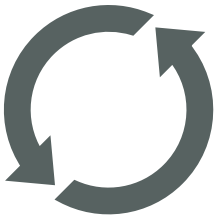
7 Hinweise

zum sicheren Verhalten am Computer

In diesem Dokument haben wir (ohne Anspruch auf Vollständigkeit) sieben einfach umzusetzende Tipps für Anwender zusammengestellt, die für mehr Sicherheit am Computer sorgen. Bei Fragen helfen wir gern weiter!

Als regional aufgestelltes IT-Systemhaus in der Region Braunschweig, Wolfsburg, Hannover betreuen wir seit 17 Jahren kleine und mittelständische Unternehmen nach dem Leitspruch „So läuft IT". Eckpfeiler unseres Portfolios sind die Themen Infrastruktur, Virtualisierung, Hardware, Kommunikation (Groupware), Schulserver, Storage, Security & Backup, Client Management sowie Helpdesk & Monitoring.

1. Updates installieren



Achten Sie darauf, dass Ihr Betriebssystem und die Software, die Sie benutzen, immer auf dem neuesten Stand sind. Insbesondere die Windows-Updates schließen häufig Sicherheitslücken.

2. Programme gewissenhaft installieren

Wenn Sie Programme herunterladen möchten, tun Sie das am besten ausschließlich von der Webseite des Herstellers. Nur so können Sie sicher sein, dass es sich um das gewünschte Programm handelt. Achten Sie bei der Installation darauf, keine unnötige Software, wie z.B. Toolbars, mit zu installieren. Diese kann ebenfalls Sicherheitslücken aufweisen und beeinträchtigt vor allem die Geschwindigkeit Ihres Browsers.

3. Datensicherung beachten

Speichern Sie alle Dokumente, mit denen Sie arbeiten, auf dem Server - keinesfalls ausschließlich auf Ihrem PC. Falls der PC kaputt geht oder von einem Virus befallen wird, bleiben die Dateien auf dem Server gespeichert und werden dort durch regelmäßige Backups gesichert. Vermeiden Sie möglichst die Benutzung von Cloudspeicher-Diensten wie z.B. Dropbox - diese Dienste können große Sicherheitslücken aufweisen.

4. E-Mail-Viren keine Chance geben

Um sich vor E-Mail-Viren zu schützen, sollten Sie einige grundsätzliche Dinge beachten: Wenn Sie Mails mit Anhängen öffnen, achten Sie darauf, keine Programme (Dateien mit der Endung .exe) auszuführen. Falls eine Datei, die Sie öffnen, nach Berechtigungen fragt, lassen Sie diese nicht zu - so könnten Viren auf Ihren PC gelangen.

SO LÄUFT IT.

LINET Services GmbH ▪ Cyriaksring 10a ▪ 38118 Braunschweig
Tel.: 0531 180508-0 ▪ Fax: 0531 180508-29 ▪ info@linet-services.de ▪ www.linet-services.de

Sollten sich Links in einer Mail befinden, öffnen Sie diese nur, wenn Sie dem Absender vertrauen bzw. er seriös erscheint und nachdem Sie die URL auf Rechtschreibfehler kontrolliert haben. So vermeiden Sie, auf gefälschte Webseiten zu gelangen (z.B. www.wicipedia.org statt www.wikipedia.org).

Kettenbriefe sollten generell nie weitergeleitet werden, sie dienen nur der Verbreitung Ihrer Mailadresse, wodurch Sie weiteren Spam erhalten.

Viele Spam-E-Mails erkennt man schon am Absender oder Betreff, dennoch sollten Sie bei unbekannten Absendern grundsätzlich sehr vorsichtig mit Anhängen oder verlinkten Webseiten umgehen.

5. Browser gewissenhaft nutzen

Auch im Browser sollten Sie darauf achten, was Sie anklicken und was nicht. Pop-Ups sind kleine Fenster, die sich - sofern man es nicht in den Browsereinstellungen ausgestellt hat - automatisch öffnen. Viele dieser Pop-ups wollen Sie durch Tricks dazu bewegen, irgendetwas herunterzuladen oder private Daten preiszugeben (z.B. *„Achtung, Ihr PC ist gefährdet! Klicken Sie hier um den KOSTENLOSEN Virenscanner herunterzuladen!“*). Solche Browsermeldungen sollten Sie stets ignorieren.

Auch mit Ihren privaten Daten sollten Sie vorsichtig umgehen: Geben Sie Name, Adresse und E-Mail-Adresse nur an, wenn Sie absolut sicher sind, dass es sich um eine seriöse Webseite handelt. Je öfter Sie Ihre Mailadresse im Internet angeben, desto mehr unerwünschte Spam-Mails werden Sie erhalten. Das lässt sich vermeiden, indem Sie sich eine oder mehrere zusätzliche Mailadressen erstellen, die Sie für Anmeldungen auf Webseiten benutzen.

Besonders vorsichtig sollten Sie mit Ihren Bankdaten umgehen. Außer beim Online-Banking müssen Sie niemals eine PIN oder Ihr Online-Banking-Passwort eingeben und die Geheimzahl Ihrer Bankkarte dürfen Sie generell unter keinen Umständen preisgeben. Um zu verhindern, dass Sie auf einer gefälschten Online-Banking-Webseite landen, geben Sie die URL immer manuell ein oder speichern diese als Lesezeichen. Benutzen Sie keine Verlinkungen.

6. Passwort ändern

Ihr Passwort ist am sichersten, wenn es regelmäßig geändert wird, möglichst lang ist und verschiedene Zeichen enthält (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen). Lange Wörter oder kurze Phrasen eignen sich gut in Kombination mit Zahlen und mindestens einem Sonderzeichen. Hierbei ist noch zu beachten, dass das Passwort nichts mit Ihrem Privatleben zu tun hat (z.B. Geburtsdaten oder Namen) - es sollte bestenfalls völlig wahllos ausgedacht sein (z.B. *„$13ZiegentanzenimGarten!“*, bitte benutzen Sie dieses Beispiel nicht). Idealerweise teilen Sie jedem Dienst ein eigenes Passwort zu. Bei der Verwaltung von Passwörtern kann ein Passwort-Manager helfen.

In unserem Blog - dieser Link ist selbstverständlich ungefährlich - erfahren Sie mehr darüber: https://www.linet-services.de/passworttipps

7. Sonstiges

Schließen Sie keine unbekannten Wechseldatenträger (USB-Sticks, CDs) an Ihren Rechner an, diese könnten absichtlich von Kriminellen verschickt oder einfach auf der Straße liegengelassen worden sein, in der Hoffnung, dass sie jemand findet und an seinen PC anschließt.

Um zu verhindern, dass Unbefugte Ihre Daten lesen oder bearbeiten können, stellen Sie sicher, dass Ihr Computer immer gesperrt ist, sobald Sie Ihren Arbeitsplatz verlassen.