ITdental

IT Profi für Ihre Dentalpraxis

Ten Rules of IT Security

was tun

was meiden

worauf achten

was melden

sicher bleiben

IT dental GmbH | Rämsiweg 4 | 6048 Horw (LU) | Schweiz | Telefon 041 342 01 54 | Mobile 079 916 10 06
info@it-dental.ch | www.it-dental.ch

1 Erkennen Sie Datendiebe

00110001

Ignorieren Sie Anfragen per Telefon oder E-Mail, die vertrauliche Informationen aus Ihrer Praxis abschöpfen wollen. Das gilt für Geheimnisse ebenso wie für Geschäftsergebnisse oder Mitarbeiterdaten.
Datendiebe versuchen oft, sich als Mitarbeiter oder Geschäftspartner auszugeben. Bleiben Sie stets wachsam, um solche Versuche frühzeitig zu erkennen, und melden Sie jeden begründeten Verdacht an Ihren IT-Supporter. Geben Sie auch Ihre eigenen, persönlichen Daten niemals leichtfertig preis.

Arbeiten Sie nicht mit ungeschützten Computern

2

00110010

Spielen Sie stets die aktuellen Sicherheitsupdates ein. Achten Sie darauf, dass eine Virenschutzsoftware und eine Firewall installiert sind. Melden Sie sich, wo immer es geht, mit den Rechten eines normalen Benutzers an –nicht mit Administratorrechten.

3 Lassen Sie sensible Daten nicht herumliegen

00110011

Ausdrucke und Merkzettel mit privaten oder sensiblen Daten sollten nicht offen auf dem Schreibtisch liegen. Verschliessen Sie die Dokumente lieber in einer Schublade oder verwenden Sie den Aktenvernichter. Dann sind sie sicher.

Halten Sie Ihren Schreibtisch in Ordnung und sperren Sie alle Dokumente stets weg. So bleiben Informationen vertraulich. Und es sieht ordentlicher aus.

Sperren Sie Ihren Computer, wenn Sie Ihn nicht benutzen

4

00110100

Denken Sie daran, den Computer zu sperren, sobald Sie Ihn nicht mehr verwenden – oder stellen Sie am besten gleich eine automatische Sperrung ein. Ihre Arbeit ist wichtig und wir wollen sicherstellen, dass Ihre Daten und Dokumente vor allen neugierigen Blicken sicher sind.

5 Bleiben Sie wachsam und melden Sie jeden Verdacht

00110101

Melden Sie verdächtige Aktivitäten immer Ihrem IT-Supporter. Denn es gehört zu unserer Aufgabe, die Computer vor Angriffen zu schützen und Datenverlust zu verhindern. Gemeinsam geht das besser. Je früher wir von verdächtigen Vorfällen oder möglichen Problemen erfahren, desto besser können wir reagieren.

Schützen Sie Daten und Geräte per Passwort

6

00110110

Schützen Sie Ihre sensiblen Daten stets mit einem starkem Passwort. Mobile Geräte wie Computer, Smartphones, USB-Sticks gehen schnell mal verloren. Nur wenn die enthaltenen Daten passwortgeschützt sind, haben Unbefugte keine Chance, die vertraulichen Daten auszulesen.

7 Wählen Sie komplexe Passwörter

00110111

Meiden Sie Allerweltspasswörter wie „Kennwort" oder „Katze", denn diese lassen sich allzu leicht erraten. Vermeiden Sie auch Muster auf der Tastatur, etwa Tastenfolgen wie „12345" oder „asdfg". Viel sicherer sind komplexe Passwörter*: Verwenden Sie dazu große und kleine Buchstaben, aber auch Ziffern, Satz- und Sonderzeichen. Verwenden Sie für jede Webseite und jeden Computer ein eigenes Passwort. Sollte ein Konto gehackt werden, sind die anderen dann trotzdem noch sicher.

Wo früher fünf bis sieben Zeichen ausreichten, sollten sich die Passwörter inzwischen langsam den zehn Stellen nähern. Schuld daran ist vor allem der massive Zuwachs an Rechenleistung, sowohl bei den CPUs wie auch den Grafikkarten. Denn mit Hilfe dieser Leistung werden Passwörter im Brute-Force-Verfahren geknackt.

*@chtZsiG! (Acht Zwerge stehen im Garten !)

Schützen Sie Daten und Geräte per Passwort

8

00111000

Geben Sie am besten niemals Ihrer Neugier nach. Löschen Sie verdächtige E-Mails lieber ungelesen und ignorieren Sie alle Links. Ein Klick auf schädliche E-Mails oder die darin angezeigten Links reicht aus, um Ihren Computer zu infizieren. Das geschieht ohne weiteres Zutun, oft ohne dass Sie davon etwas bemerken.

Gute Faustregel: Klingt ein Angebot zu schön, um wahr zu sein, steckt mit einiger Sicherheit ein Betrug dahinter.

9 Schliessen Sie persönliche Geräte nur nach Erlaubnis an

00111001

Schliessen Sie persönliche Geräte wie USB Flash-Laufwerke, MP3-Player oder Smartphones nicht ohne die Erlaubnis Ihrem IT-Supporter am Computer an.

Der Grund: Befindet sich versteckter Schadcode auf dem Gerät, wird er beim Anschliessen sofort automatisch ausgeführt. Sprechen Sie daher Ihre Gerätenutzung stets mit dem IT-Supporter ab. Entscheiden Sie in diesem Fall lieber nicht selbst.

Schützen Sie Daten und Geräte per Passwort

10

00110001
00110000

Schadprogramme und Spionagetools verstecken sich oft in vermeintlich normalen, harmlosen Anwendungen, etwa Spielen, Tools, sogar in Virenschutzsoftware.

Angreifer versuchen, Sie auf diesem Weg zu überlisten, um über Ihren Computer in das Unternehmensnetzwerk einzudringen.

Sie wollen trotzdem ein bestimmtes Programm nutzen? Sprechen Sie einfach den IT-Supporter darauf an, damit er es für Sie prüfen kann.

Bleiben Sie wachsam!

Solange es Daten gibt, wird es Angreifer geben, die diese stehlen oder zerstören wollen. Dabei wird es immer neue Tricks geben, so dass auch diese zehn Tipps sich künftig verändern werden.

Wir aktualisieren dieses Handbuch „Ten Rules of IT Security" regelmässig. So sorgen wir dafür, dass Sie und Ihre Praxis auch weiterhin sicher arbeiten können.

Mein Name ist Fabian Brülhart, was kann ich für Sie tun?

IT dental GmbH | Rämsiweg 4 | 6048 Horw (LU) | Schweiz | Telefon 041 342 01 54 | Mobile 079 916 10 06
info@it-dental.ch | www.it-dental.ch