

# Top 10

## Security Tips für Netzwerkbenutzer

*Bei und nach Untersuchungen haben IT-Administratoren herausgefunden, dass die stärkste Bedrohung gegen ihr Netzwerk durch die eigenen Kollegen herbeigeführt wird. Erzielen Sie über die folgenden 10 Hinweise Einigkeit mit Ihren Netzwerkbenutzern und es wird sich sofort als „Netzwerksicherheit“ bezahlt machen.*

### 1. **Misstrauen Sie unerwarteten Brieffreundschaften.**

Die meisten Computerviren werden durch das Öffnen von Email-Anlagen eingefangen. Moderne Viren können fälschlicherweise Namen von Bekannten annehmen und als Absender der Email auftreten. Wenn ein Anhang unerwartet zugesendet wird, vergewissern Sie sich bei ihrem Bekannten über die Richtigkeit, bevor sie den Anhang öffnen.

### 2. **Sei ein Anti-Virus-Fan.**

Halten Sie Ihre Anti-Virus-Software immer auf dem neuesten Stand, und verwenden Sie diese auf allen Computern. Benutzen Sie Software, die sich automatisch auf dem neuesten Stand hält, damit Sie eine Nasenlänge voraus bleiben.

### 3. **Benutzen sie komplizierte Passwörter.**

Hacker arbeiten mit Programmen, die automatisch alle Wörter eines Lexikons als ihre mögliche Passwörter verwenden. Verwenden Sie lange, schwer zu ermittelnde Passwörter, die eine Mixtur von Buchstaben, Ziffern und Sonderzeichen enthalten. Um sich solche Passwörter einzuprägen, benutzen Sie Zeilen aus einem Gedicht, Lied oder einem Filmtitel.

### 4. **Heben sie Passwörter nie in Schriftform auf.**

Mehr und mehr Diebe stehlen Computerdaten oder Belege aus den Häusern ihrer Opfer. Notizen und Sticker am Arbeitsplatz die Passwörter, Mitgliedsnummern oder andere vertrauliche Informationen enthalten, machen es Dieben zu einfach. Vernichten Sie solch unterstützendes Material.

### 5. **Achten sie auf Schnüffler.**

Passen Sie auf, dass Schnüffler Ihren Computer nicht während ihrer Abwesenheit untersuchen können. Auf Windows-Systemen drücken sie Strg-Alt-Entf, dann wählen sie „Computer sperren“.

#### PASCAL BERATUNGSGESELLSCHAFT FÜR DATENVERARBEITUNG MBH

Mörkenstraße 5, 22767 Hamburg  
Postfach 50 12 44, 22712 Hamburg  
Telefon 0 40 / 3 06 11-0  
Telefax 0 40 / 3 06 11-236  
E-Mail info@pascal.de  
Internet http://www.pascal.de

Geschäftsführer:  
Dipl.-Kfm. Peter Hansen  
Maria Hansen  
Lars Lübcke  
Dipl.-Ing. Kurt Wiechmann  
Handelsregister Hamburg Reg.-Nr. B 21298  
USt. Id. Nr. DE 118 587 498

Deutsche Bank Hamburg  
(200 700 00) 6 464 499  
Hamburger Sparkasse  
(200 505 50) 1037/211 156  
Commerzbank Hamburg  
(200 400 00) 4 000 253  
Steuer-Nr. 0285 300 339 FA HH-Altona

## 6. **Drahtlos bedeutet wirklich Radio.**

Wenn Sie WLAN zu Hause betreiben, werden die Wellen durch ihre Wände nicht aufgehalten. Solange Sie keine Messungen betreiben, können sich mobile Hacker in ihr Netzwerk einschalten und von dort in das Firmennetzwerk gelangen. Fragen Sie ihren Netzwerkadministrator, welche Einträge Sie in Ihrem WAP vornehmen sollen, um unerwünschte Zugriffe zu verhindern, so dass nur Ihre eigenen MAC-Adressen die Verbindung aufbauen können.

## 7. **Bleiben sie auf sicheren Web-Seiten.**

Ihnen ist die Gefahr bewusst, wenn Sie sich in unsicheren Ecken ihrer Stadt bewegen. Web-Surfing sollten Sie genauso handhaben. Bösartige Software wird häufiger über Pornoseiten, Spiele-Seiten und Szenekulturseiten auf den Computern der Opfer installiert als über sehr bekannte Seiten. Zur Sicherheit vermeiden Sie Web-Seiten, die Sie in der Öffentlichkeit nie benutzen würden.

## 8. **Schalten sie vor jedem Click ihr Gehirn ein.**

Prüfen Sie den Link, bevor Sie ihn aufrufen. Um sicher zu sein, wohin der Link verzeigt, fahren Sie mit der Maus auf den Link und schauen sich die Adresse in der Browser-Status-Leiste an, oder Sie verwenden die rechte Maustaste und wählen Eigenschaften. Solange Sie keine Dateien downloaden wollen, sollten in der URL keine \*.exe, \*.cmd o.ä. stehen. Dies sind ausführbare Programme und können bösartig sein.

## 9. **Seien sie wählerisch.**

Überprüfen sie regelmäßig ihren Computer auf „Adware“ und „Spyware“ die irgendwelche Web-Seiten still und leise installiert haben könnten. Bevor Sie „Freeware“ downloaden, überprüfen Sie die Seriosität des Anbieters. Zum Beispiel überprüfen Sie den Anbieter mit „Google“.

## 10. **Sagen sie lieber nein.**

Wenn Sie eine Web-Seite besuchen und Sie werden gefragt, ob Sie Ihr Passwort dauerhaft speichern wollen, veröffentlichen Sie es nicht. Denn das Passwort wird auf ihrem Computer gespeichert und jedermann, der sonst Zugriff auf ihren Computer hat, kann dieses „Login“ ebenfalls benutzen.

***Haben Sie Fragen dazu, oder ist Ihnen Ihr Netzwerk zu unsicher, setzen Sie sich mit PASCAL in Verbindung, und wir werden dieses Problem zuverlässig und professionell beseitigen.***

### **PASCAL BERATUNGSGESELLSCHAFT FÜR DATENVERARBEITUNG MBH**

Mörkenstraße 5,	22767 Hamburg	Geschäftsführer:	Deutsche Bank Hamburg
Postfach 50 12 44,	22712 Hamburg	Dipl.-Kfm. Peter Hansen	(200 700 00) 6 464 499
Telefon	0 40 / 3 06 11-0	Maria Hansen	Hamburger Sparkasse
Telefax	0 40 / 3 06 11-236	Lars Lübcke	(200 505 50)1037/211 156
E-Mail	info@pascal.de	Dipl.-Ing. Kurt Wiechmann	Commerzbank Hamburg
Internet	http://www.pascal.de	Handelsregister Hamburg Reg.-Nr. B 21298	(200 400 00) 4 000 253
		USt. Id. Nr. DE 118 587 498	Steuer-Nr. 0285 300 339 FA HH-Altona