SICHER DURCH WEBHYGIENE

Die 10 Regeln der Webhygiene

1. Verwenden Sie mehrere und auch sichere Kennwörter

- Ein sicheres Kennwort besteht mindestens aus 10-16 Zeichen, darunter große und kleine Buchstaben, Zahlen und Sonderzeichen.
- Das Kennwort sollte nicht in Verbindung mit Ihnen stehen d.h. verwenden Sie keine Namen von Freunden.
- Trennen Sie privat von beruflich und verwenden Sie im Job nicht das gleiche Passwort wie bei der privaten Nutzung von Diensten im Internet.

2. Halten Sie den Virenschutz am Computer aktuell und eingeschaltet

- Bestimmte Viren und Trojaner verteilen Ihre Daten per Upload im Internet.
- Ein Virenschutz ist daher Pflicht für einen Computer, aber halten Sie diesen auch aktuell.
- im Job: Melden Sie ungewöhnliches Verhalten des PCs dem Systemadministrator.

3. Nutzen Sie soziale Netzwerke privat nur mit Pseudonym

- Ein Pseudonym („Fake-Name“) schützt den echten Namen – insbesondere in sozialen Netzwerken wie z.B. Facebook oder StudiVZ.
- Die Reputation ist dem Pseudonym weitestgehend (Ausnahmen !) geschützt.
- Freunde gewöhnen sich an das Pseudonym.

4. Seien Sie sparsam mit Bildern im Internet

- Profilbilder (Darstellung des kompletten Gesichts) sind zu vermeiden.
- Sepia-/Graustufen-Bilder schützen Sie – im Moment noch – vor „Nacktpixelscannern“ im Internet.
- Empfohlene Bildgröße: max. 320 x 240 Pixel.

5. Vermeiden Sie identifizierende und persönliche Angaben im Internet

- Löschen Sie Geburtsdatum, eMailadresse, Postanschrift aus Profil und Chronik.
- Schalten Sie Ortungsfunktionen via Handy ab, denn sie ermöglichen weltweite Verfolgbarkeit.

6. Prüfen Sie Ihre Freundesliste in sozialen Netzwerken regelmäßig

- Prüfen Sie einmal bis zweimal jährlich die Freundesliste und dünnen Sie diese aus.
- Stellen Sie sich hierbei die Frage: „Kann ich diese Person auch im richtigen Leben erreichen?“
- Löschen Sie „Einmalfreundschaften“ und prüfen Sie, ob ein Freund vielleicht doppelt angezeigt wird.
- Schalten Sie die Anzeige der eigenen Freundesliste ab.

7. Halten Sie die Chronik in sozialen Netzwerken so kurz wie möglich

- Die Chronik speichert Ihre Daten sehr lange, daher ist diese von Zeit zu Zeit zu leeren.
- Senden Sie keine geheimen Daten über die Chronik und die Nachrichten-Funktion.

8. Kontrollieren Sie regelmäßig die Privatsphäre-Einstellungen der genutzten Dienste

- Von Zeit zu Zeit ändern soziale Netzwerke die Privatsphären-Einstellungen – meist ohne Vorwarnung.
- Die Verwendung von komplizierten Datenverwendungsbedingungen, doppelten Verneinungen oder widersprüchlicher Aussagen machen ein aufmerksames Lesen der Bedingungen notwendig.
- Facebook: Abonnieren Sie die Seite „Facebook Site Governance“ – sie enthält Änderungen bei Facebook.

9. Verweigern Sie Apps oder Spielen den Zugriff auf die persönlichen Daten

- Verweigern Sie Apps oder Spielen den Zugriff auf Ihre Freundesliste oder das Adressbuch.
- Zudem verraten Spiele, wie Sie die Freizeit nutzen. Hierfür interessieren sich womöglich auch Arbeitgeber.

10. Begehen Sie keine Rechtsverletzungen

- Illegale Down- und Uploads können Abmahnungen und/oder Unterlassungserklärungen zur Folge haben.
- Das Bloßstellen von Personen im Internet („Cybermobbing“) kann strafrechtliche Folgen haben.
- Achten Sie das „Recht am eigenen Bild“, d.h. ungefragt sollten Sie keine Bilder von Personen oder Personengruppen ins Internet stellen.

Diese Tipps und weitere Informationen finden Sie auch unter www.webhygiene.de.

Karriere-Studio Holger Weber | Projekt Webhygiene | Goethestraße 16 | 63834 Sulzbach | info@webhygiene.de