Thomas Czok
IT-Trainer Verbraucherbildung Bayern

Verhaltenstipps für den sicheren Umgang im Internet

1. **Verwenden Sie ein aktuelles Betriebssystem und stellen Sie sicher, dass alle zur Verfügung stehenden Updates eingespielt wurden.**

   Die meisten Softwarehersteller schließen bekannt gewordene Sicherheitslücken schnell und verteilen die Updates über das Internet.

2. **Verwenden Sie zum Surfen im Internet nur Browser mit aktuellen Versionsständen**

   Veraltete Internetbrowser stellen ein hohes Sicherheitsrisiko dar. Neue Versionen sind in der Regel ausgereifter und sicherer.

3. **Löschen Sie regelmäßig Ihre Browser Cookies**

   Viele Seiten benötigen Cookies um richtig funktionieren zu können, das ist OK. Löschen Sie dennoch in regelmäßigen Abstanden die Cookies aus dem Browser.

4. **Löschen Sie regelmäßig den Browserverlauf und den Browsercache.**

   Sollte jemand Zugriff auf Ihren PC erhalten, könnte er sich ein umfangreiches Bild Ihrer Internetaktivitäten machen.

5. **Legen Sie sich mind. eine zweite E-Mail-Adresse zu, die Sie nur für „unwichtige“ Registriervorgänge verwenden.**

   Verwenden Sie für Bezahlvorgänge, Bestellungen und zum Registrieren in Foren usw. mehrere verschiedene E-Mail-Adressen. Eine gute Möglichkeit in diesem Zusammenhang sind auch sog. Minutemail-Anbieter wie zum Beispiel 10minutemail.com, my10minutemail.com, wegwerfmail.de, trash-mail.com.

6. **Füllen Sie im Rahmen von Bestellungen usw. bei Webformularen nur die unbedingt notwendigen Pflichtfelder aus**

   Oftmals werden weitergehende Angaben abverlangt, die mit dem eigentlichen Bestellvorgang in keinem Zusammenhang stehen. Warum sollten Sie diese Daten freiwillig von sich preisgeben?

7. **Beachten Sie die Pflichtfelder genau und überlegen Sie, ob alle Ihrer Eingaben immer der Wahrheit entsprechen müssen.**

   Sollte das Geburtsdatum als Pflichtfeld vorhanden sein, überlegen Sie bitte, ob die Eingabe eines „alternativen" Geburtsdatums Nachteile bringen würde.

8. **Gehen Sie grundsätzlich sehr sparsam mit Ihren Daten um**

   Alle Daten die Sie im Internet hinterlassen, lassen sich nicht mehr löschen und bleiben für immer dort gespeichert. Machen Sie sich das bewusst, bevor Sie Daten aller Art ins Internet stellen.

9. **Verwenden Sie in Diskussionsforen niemals Ihren richtigen Namen, sondern ein Pseudonym.**

   Dieses Vorgehen ist absolut üblich und wird bei den meisten Registrierungsvorgängen auch aktiv beworben.

10. **Achten Sie bei Kommentaren, Rezessionen und Beiträge aller Art darauf, keine persönlichen Daten preiszugeben**

    Nach Inhalten von Foren, Beiträgen oder auch Rezessionen kann zielgerichtet recherchiert werden. Ein Rückschluss auf Ihre wahre Identität könnte, z. B. bei medizinischen Daten, unangenehme Folgen haben.

11. **Überlegen Sie genau, welche Daten Sie in der „Cloud" ablegen. Dazu gehören auch Daten von Fitnesstrackern, Runstatic usw.**

    Gehen Sie davon aus, dass alle Daten, die Sie irgendwo im Internet ablegen, grundsätzlich auch verwertet werden können. Auch wenn nicht immer kriminelle Interessen ausschlaggebend sind, spielen dennoch oftmals monetäre Gründe eine Rolle. Ihre Daten sind bares Geld wert – Gesundheitsdaten erste recht!

12. **Posten Sie möglichst wenig persönliche Fotos von Sich oder Ihren Kindern in den Sozialen Medien. (Merke: Poste nur Sachen, die Sie auch Ihrer Oma zeigen würden)**

    Einmal in das Internet eingestellte Fotos bleiben immer vorhanden. Gerade bei Kindern und Jugendlichen kann dies bei der späteren Berufsauswahl zu erheblichen Problemen führen. Die meisten Personalsachbearbeiter nutzen Internetrecherchen um sich ein Bild von Ihren Kandidaten zu machen.

13. Zahlen Sie, wenn möglich, nicht mit Kreditkarte. Nutzen Sie alternative Zahlungsmethoden (z.B. PayPal)

Das Zahlen mit Kreditkarten stellt immer ein gewisses Risiko dar. Auch wenn man Zahlungen rückgängig machen lassen kann, bedarf dies doch einer ständigen Kontrolle. Besser ist es, geschlossene System wie z. B. PayPal zu nutzen.

14. Vermeiden Sie den Einsatz von Bonuskarten aller Art.

Bonuskarten sind sehr weit verbreitet. Dadurch wird Ihr Einkaufsverhalten analysiert und Ihnen z. B. zielgerichtet Werbung unterbreitet. Vergleiche haben gezeigt, dass z. B. Supermärkte ohne Bonuskarten oftmals günstiger sind.

15. Überprüfen Sie die Datenschutzeinstellungen Ihres Mobiltelefons und Ihres Internet-Browsers

Google verfolgt Sie. Haben Sie zum Beispiel den Google Standortverlauf aktiviert, werden Ihre GPS-Daten an Google gesendet und ein ausführliches Bewegungsprofil von Ihnen erstellt.

16. Öffnen Sie keine E-Mail-Anhänge von unbekannten Absendern

Seien sie vorsichtig bei Dateianhängen aus unbekannten Quellen und in den Formaten pdf, zip. exe

17. Sehen Sie sich in der Statusleiste im Verdachtsfall die genaue Zieladresse eines Links an.

Nehmen Sie sich die Zeit und sehen sie sich die Statusleiste am unteren Browserfenster an. Hier wird das Ziel des Links angezeigt. Sie werden sich wundern, wo manche Aufforderungen zum „Hier Klicken“ hinführen. Achten Sie hier explizit auf die Top-Level Domain Bezeichnung. (z.B. DE/ORG/RU)

18. Lesen Sie Internetadressen immer von rechts nach links.

Es sind immer wieder gute Phishing-Seiten im Umlauf, die sich von den echten Seiten nicht oder nur ein wenig unterscheiden. Hier werden Sie gebeten Ihre Zugangsdaten einzugeben. Das Ziel dieser Seite erkennen Sie nur, wenn Sie die Zieldomain genau ansehen. (www.spasskasse.de, www.amazon.hackerseite.de)

19. Verwenden Sie unterschiedliche Passwörter für unterschiedliche Bereiche

Die Nutzung eines einzigen Passwortes für unterschiedliche Bereich ist mehr als fahrlässig. Ist diese einmal bekannt geworden oder gehackt, hat der Angreifer Zugang zu alle Ihren Daten.

20. Ändern Sie umgehend alle Standardpasswörter (Telefon, Router, IP-Cam)

Die meisten Geräte werden mit Standardpasswörter ausgeliefert. Diese Passwörter sind bekannt. Wer Zugriff auf Ihr Gerät über das Internet hat, hat somit die volle Kontrolle darüber.

21. Ihr E-Mail Passwort ist wahrscheinlich das wichtigste Passwort das Sie haben. Achten Sie hier auf ein sicheres Passwort.

Nehmen Sie sich einmal bewusst die Zeit und überlegen, was passieren könnte, wenn ein Hacker Ihr E-Mail Passwort hätte. Richtig: Er könnte von allen mit dieser E-Mail eingerichteten Konten die Passwörter ändern und in Ihrem Auftrag Einkaufen. Sie wären pleite!

22. Speichern Sie Passwörter nicht auf dem Computer, oder in der Cloud ab

Auch wenn davon auszugehen ist, dass seriöse Cloud-Anbieter Ihre Daten nicht sichten, kann niemand versichern, dass nicht einzelnen Personen in den Rechenzentren kriminelle Gedanken haben. Richtig sensible Daten gehören nicht in die Cloud

23. Legen Sie notierte Passwörter nicht an zugänglichen Stellen ab.

Das Passwort unter der Tastatur oder im Geldbeutel birgt ein erhebliches Sicherheitsrisiko

24. Bleiben Sie ruhig und gelassen, sollten Sie E-Mails mit Zahlungsaufforderungen bekommen. Im Zweifelsfall holen Sie sich professionelle Hilfe (Verbraucherzentralen, Polizei, Infoseiten im Internet)

Sollte Sie Zahlungsaufforderungen bekommen, bleiben Sie ruhig, sehen Sie sich die Mail genau an, überprüfen Sie die Links und recherchieren Sie im Internet nach dem Betreff. Oftmals werden Sie feststellen, dass diese Mails schon bekannt sind und auch davor gewarnt wird.

Nützliche Links im Internet:

http://www.computerbetrug.de

https://www.sicher-im-netz.de

http://www.klicksafe.de

https://www.bsi-fuer-buerger.de

www.verbrauchertrainer-bayern.de

https://www.phishtank.com/