Die große Sicherheits-Checkliste fürs Internet

Ob bei Google, Facebook, Amazon oder eBay – jede Aktion hinterlässt Spuren. Werden diese Daten erst einmal zu einem personenbezogenen Profil zusammengefasst, sind sie kaum noch zu löschen. Diese Regeln helfen, das virtuelle Internet-Ich zu verwischen und sicher zu surfen

// Wie sichere ich mein WLAN richtig?

Wer per Funk mit dem Internet verbunden ist, sollte sein WLAN-Signal (Wireless Local Area Network) unbedingt verschlüsseln. Sonst können Hacker die Daten abfangen oder Ihren Internetzugang für illegale Aktivitäten (z. B. Downloads) nutzen. Wichtig: Ihr Passwort sollte mindestens 20 Zeichen lang sein. Wie die WLAN-Verschlüsselung aktiviert wird, steht im Handbuch des Internetrouters. Die sicherste Verschlüsselungsvariante für den privaten Bereich ist derzeit WPA2.

// Wie google ich, ohne zu googeln?

Google ist Weltmeister im Datenspeichern – jedes Wort, jede Suche wird nebst IP-Adresse abgespeichert. Datenschützer empfehlen daher Ixquick, Startpage oder Startingpage. Diese Suchmaschinen verzichten auf jegliche Archivierung von IP-Adressen und Nutzerdaten. Zudem wird jede Suchanfrage anonymisiert – und erst dann an die gewünschten Webseiten weitergeleitet.

// Wie registriere ich mich im Web, ohne meine E-Mail-Adresse anzugeben?

Wer Internetangebote nutzen will, muss sich in der Regel registrieren. Gibt man jedoch seine private E-Mail-Adresse an, leidet die Anonymität. Die Folge: Lästige Spam-Attacken. Web-Dienste wie trashmail.com, spambog.com, sofort-mail.de oder mailinator.com dagegen bieten gratis Mail-Adressen, die keine Registrierung verlangen und sich somit spontan einsetzen lassen. Zudem werden keinerlei Daten abgefragt, die Anonymität bleibt also erhalten. Diese Wegwerf-Postfächer

dienen allerdings nur zum Empfangen, nicht zum Versenden von E-Mails.

// Wie lösche ich den Spion in meinem PC?

IT-Experten haben gerade 3180 Spähdateien auf 50 populären Webseiten gefunden, darunter auch bei eBay. Diese Cookies nisten sich heimlich während einer Internetsitzung ein und speichern alle angeklickten Artikel und Vorlieben. Firmen wie Rapleaf werten diese Cookies im Auftrag von Suchmaschinen oder sozialen Netzwerken anschließend aus – oft mit Namen und E-Mail-Adressen. Diese Datenprofile werden dann z. B. für den Spam-Versand benutzt. Sicherheitsexperten und Verbraucherschützer empfehlen daher, die Cookies regelmäßig zu löschen. Ausführliche Anleitung unter: www.verbraucher-sicher-online.de/thema/cookies.

// Wie surfe ich anonym im Netz?

Wer sich durchs Web bewegt, hinterlässt immer eine elektronische Spur, die sogenannte IP-Adresse (IP = Internet Protokoll) – durch die Wahl der Webseiten, durch das Ankreuzen von Vorlieben. Auf der Basis dieser Daten erstellen Google, eBay oder Facebook präzise Profile, die sie verkaufen – z. B. an Werbeunternehmen. Mit kostenlosen Programmen wie CyberGhost VPN oder JAP von der Technischen Universität Dresden können Nutzer jedoch anonym und legal unbeobachtet im Internet surfen (anon.inf.tu-dresden.de).

// Wie sieht ein sicheres Passwort aus?

Das Bundesamt für Sicherheit in der Informationstechnik rät: Ein Passwort sollte mindestens acht Zeichen haben (Ausnahme: WPA2, s. o. l.). Wichtig: Verwenden Sie nie Namen von Familienmitgliedern, einfache Ziffern (123abc) oder die üblichen Sonderzeichen (&!?). BSI-Tipp: Ein Passwort ist leichter zu merken, indem man sich einen Satz ausdenkt, von jedem Wort nur den ersten Buchstaben nimmt und bestimmte Buchstaben durch Zahlen oder Sonderzeichen ersetzt. Beispiel: „Jeden Samstag sehe ich die Sportschau". Die ersten Buchstaben: „JSsidS". „i" sieht aus wie „1", „$" ersetzt das „S": „JSs1d$".

// Was ist beim Internet-Einkauf zu beachten?

Deutsche Gerichte setzen mittlerweile ein Mindestmaß an Kenntnissen über die Sicherheit im Netz voraus. Dazu gehört z. B. das Erkennen von Internetadressen, die eine verschlüsselte Übertragung garantieren. Ansonsten werden beim Onlinebanking oder -einkauf entstandene Schäden in der Regel auch nicht ersetzt. Daher rät das BSI: Bankdaten, Kredit- oder EC-Kartennummer nur über verschlüsselte Verbindungen nutzen – meist erkennbar am „https://" statt des „http://" in der Adresszeile. Oft wird in der Adressleiste zusätzlich ein Schlosssymbol angezeigt. Informationen zur Verschlüsselung erhält man übrigens mit einem Klick auf das Schlosssymbol. Sie ist ausreichend, wenn diese Zahl nicht unter „128 Bit" liegt.

// Welche Gefahr lauert hinter Link-Kürzeln wie tinyurl.com?

Kürzeldienste wie tinyurl.com schrumpfen Webadressen auf ein kompaktes Maß. So lassen sich Links verschicken, ohne die beschränkte Zeichenlänge bei Xing oder Twitter zu sprengen. Immer häufiger verbergen sich hinter solchen Kürzeln Phishing-Seiten. Tipp: Wer gratis Browsererweiterungen wie Power Twitter installiert, bekommt die vollständige Webadresse angezeigt. Enthalten diese das „@"-Zeichen oder Endungen wie „com.ro" oder „com.tv", stecken in der Regel Kriminelle dahinter.