Infoblatt: Risiken

Was könnt ihr tun, um euch gegen Schadprogramme, Ausspähen oder Tracking zu schützen?

Risiken auf Websites

Viele Webseiten versuchen, euer **Nutzungsverhalten** über mehrere Plattformen hinweg zu verfolgen. Sie beobachten euren **Browser**, euren **Standort** und andere **Nutzungsdaten**, um herauszufinden, wo ihr seid und wann ihr auf die Webseiten zugreift.

Stellt euch folgende Fragen: Welchen Nutzen habe ich davon, wenn meine Handlungen verfolgt werden? Was ist mir meine Privatsphäre wert? Wie sehr möchte ich diese Inhalte ansehen?

Seid vorsichtig, wenn ihr auf Links, Werbung oder Social-Media-Beiträge klickt. Entspricht die **URL** der erwarteten Adresse? Erscheint dieselbe Seite, wenn ihr die Adresse selbst eintippt oder danach sucht? Wenn ihr im Internet surft, können böswillige Hacker*innen ebenso Daten über euch sammeln wie Internetanbieter*innen. Um dieses Risiko zu senken, müsst ihr eine sichere Verbindung zwischen euch und der Webseite herstellen, auf die ihr zugreifen möchtet.

HTTPS ist ein Standard, den Webseiten für die Verschlüsselung von über das Internet gesendeten Daten verwenden. Die Abkürzung steht für „Hypertext Transfer Protocol Secure“, übersetzt: „**Sicheres Hypertext-Übertragungsprotokoll**“. Das bietet eine zusätzliche Sicherheitsebene und kann in jedem Browser verwendet werden, indem am Anfang der verwendeten URL „**https://**“ eingefügt wird. HTTPS wird jedoch nicht von allen Website-Angeboten unterstützt.

1. Vertrauliche Informationen (z. B. Passwörter und Kreditkartendaten) solltet ihr nur auf Webseiten mit dem Präfix HTTPS:// eingeben.
2. Mit Software-Tools könnt ihr festlegen, dass immer HTTPS verwendet wird, wenn möglich.
3. Die meisten gängigen Browser weisen mit einem Schloss-Symbol neben der Adressleiste auf eine sichere HTTPS-Verbindung hin.
4. Auch HTTPS heißt nicht, dass eure Informationen sicher sind. HTTPS sichert die Verbindung, also den Weg zur Website. Die Website selbst kann trotzdem bösartig sein.

EV-Zertifikate erhalten Webseiten, die ihre Identität gegenüber einer Zertifizierungsstelle bestätigen. In Browsern wird als EV-Nachweis manchmal der Name der Seite oder der Zertifizierungsstelle neben der Adressleiste angezeigt. Wenn euch die Inhalte auf einer bestimmten Website verdächtig vorkommen, könnt ihr überprüfen, ob die URL im Zertifikat mit der URL im Browser übereinstimmt, indem ihr auf „Zertifikat anzeigen“ klickt.

Risiken durch Schadprogramme

Schadprogramme können Daten von eurem Computer sammeln, sie können aber auch anderen die Kontrolle über euren Computer geben. Manchmal sind es Webseiten, die sichere Portale wie die einer Bank imitieren, oder Erweiterungen, die Werbung in eurem Browser platzieren, um damit Geld zu verdienen. Ihr solltet **Software** nur von **vertrauenswürdigen Quellen** herunterladen und installieren und sorgfältig darüber nachdenken, bevor ihr ausführbare Dateien (z. B. mit der Dateiendung .exe, .pkg, .sh, .dll oder .dmg) herunterladet. Ausführbare Dateien sind Dateien, die einen bestimmten Vorgang ausführen. Manchmal handelt es sich dabei um böswillige Vorgänge. **Antiviren-Software** kann euch dabei helfen, das Ausführen von Schadprogrammen zu verhindern. Einige Antiviren-Programme sind bereits auf eurem Computer installiert, und manche Computer haben schützende Einstellungen. Denkt sorgfältig darüber nach, bevor ihr diese Einstellungen verändert. Antiviren-Software verhindert nicht nur, dass Software von unsicheren Quellen ausgeführt wird, sondern warnt euch auch davor, nicht vertrauenswürdige Seiten zu besuchen und Schadprogramme herunterzuladen.

Auch **Browsererweiterungen**, die **Plug-ins** blockieren, können hilfreich sein. So wird es beispielsweise Webseiten erschwert, eure Identität oder euren Standort herauszufinden. Das gleiche Plug-in kann jedoch auch Funktionen von Webseiten blockieren, wie zum Beispiel das Abspielen von Videos. Ob ihr Browsererweiterungen installieren möchtet oder nicht, hängt von euren Einstellungen und von den Sicherheitsrisiken ab, die ihr bereit seid, einzugehen.

Überprüft mehrmals, dass ihr über vertrauenswürdige Webseiten auf Downloads zugreift. Seid äußerst vorsichtig, bevor ihr unbekannte E-Mail-Anhänge öffnet oder auf Pop-up-Fenster und Fehlermeldungen klickt. Zudem kann es hilfreich sein, seriöse Software gegen Schadprogramme auf eurem Computer zu installieren.

Phishing und eure Passwörter

Phishing tritt meist per E-Mail auf. Jemand fragt euch nach eurem Passwort und hofft, dass ihr es ihm per E-Mail sendet oder es auf einer gefälschten Webseite eingebt. **Spamfilter** können verhindern, dass einige dieser E-Mails in eurem Postfach angezeigt werden. Um Spamfilter zu verbessern, markiert verdächtige E-Mails in eurem Postfach als **Spam**.

Ihr solltet eure Passwörter niemals mit anderen Personen teilen und sie nur für die Anwendung nutzen, bei der ihr euch anmelden möchtet. Beim **Phishing** wird versucht, jemanden durch Tricks dazu zu bringen, das eigene Passwort preiszugeben. Um Zugriff auf eure Konten zu erlangen, fragen Personen euch manchmal direkt nach eurem Passwort und behaupten, dass euer Konto gefährdet sei.

Euer Passwort an Freund*innen weitergeben?

Einige dieser Personen haben möglicherweise gute Absichten – zum Beispiel der Freund, der anbietet, sich etwas in eurem Konto anzusehen, das euch Sorgen macht. Es ist aber nicht klug, das eigene Passwort mit anderen zu teilen, besonders, wenn ihr dieses Passwort für mehrere Dinge verwendet. Das solltet ihr sowieso nicht tun. Wenn ihr euer Passwort mit anderen teilen möchtet, nutzt es nicht für andere Plattformen und nutzt einen **Passwort-Manager** für den gemeinsamen Zugriff.

Euer Passwort an Eltern weitergeben?

Manchmal sind die Personen, die nach euren Passwörtern fragen, Erwachsene, die ihr kennt und denen ihr vertraut, zum Beispiel eure Eltern. Auch wenn ihr diese Personen kennt und ihnen vertraut, ist es meistens für alle Beteiligten eine positive Erfahrung, über den Grund dieser Anfrage und den **Umgang mit euren Passwörtern** zu sprechen.

Euer Passwort an Fremde weitergeben?

Besonders Erwachsene außerhalb eurer Familie solltet ihr direkt fragen, ob es eine **gesetzliche Grundlage** gibt, die besagt, dass ihr ihnen eure Passwörter mitteilen müsst. Wenn ein Polizist oder ein Regierungsbeamter euch nach euren Social-Media-Passwörtern fragt, bleibt ruhig und respektvoll. Fragt die Person, wozu sie diese Informationen benötigt und auf welcher gesetzlichen Grundlage sie ihrer Meinung nach berechtigt ist, diese Informationen von euch zu erhalten.

In manchen Situationen kann es tatsächlich nötig sein, einem Elternteil, Lehrkräften, Polizei- oder Regierungsbeamt*innen oder anderen Erwachsenen eure Passwörter mitzuteilen. Zum Beispiel wenn eine gesetzliche Grundlage besteht, oder der Vorteil, den die Hilfe dieser Person euch bietet, eurer Meinung nach das Risiko der Passwortweitergabe wert ist.

Wenn Erwachsene, oder auch Freund*innen euch nach eurem Passwort fragen und diese Anfrage euch unangenehm ist, wendet euch sofort an eure Eltern oder eine andere erwachsene Vertrauensperson, am besten noch bevor ihr auf die Anfrage reagiert.