Medienkompetenz

Der beste Schutz gegen digitale Übergriffe ist die Vorsorge. Auch wenn Angriffe sich nicht gänzlich vermeiden lassen, können Sie durch entsprechende Absicherung das Risiko des Schadenseintritts bzw. die Schadenshöhe minimieren. Daher gilt: Wer seine technischen Geräte und persönlichen Daten absichert, ist Angriffen nicht wehrlos ausgeliefert. Auch die Rücksicht auf andere Menschen und ein solidarisches Miteinander spielen eine Rolle, denn unser Leben wird durch Kommunikation bestimmt.

Ausführliche Hinweise finden Sie u.a. auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik: https://www.bsi-fuer-buerger.de

Die nachfolgenden kurzen Orientierungshilfen können Ihnen einen sicheren und kompetenten Umgang in der digitalen Welt verschaffen.

HALTUNG UND SOLIDARITÄT

In der heutigen Zeit ist es technisch möglich und wird auch vielfach praktiziert, Daten ungefragt weiterzugeben. Ob ein Foto über Facebook, die Handynummer durch eine WhatsApp-Gruppe oder die Angabe Ihres Aufenthaltsortes durch einen Tweet, die Daten werden oftmals unreflektiert verteilt. Seien Sie hier anderen ein gutes Vorbild. Gehen Sie respektvoll mit den Daten Ihres Umfelds um, fordern Sie eine gleiche Behandlung Ihrer Daten ein und thematisieren Sie Ihre Kommunikationsentscheidungen offen.

Was können Sie tun, um für die größtmögliche Sicherheit Ihrer eigenen Daten und der Ihres Freundeskreises zu sorgen?

Geben Sie keine fremden Daten, wie die Handynummer oder E-Mail-Adresse weiter. Eine kurze Nachfrage ist nicht aufwändig.

Markieren Sie andere Menschen nicht auf Fotos bei Facebook. Laden Sie nicht einfach Fotos hoch, ohne die abgebildeten Personen um Erlaubnis gefragt zu haben.

Überlegen Sie sich, ob Sie Gruppen, wie beispielsweise WhatsApp, beitreten möchten. Dort wird Ihre Handynummer nicht nur allen Gruppenmitgliedern angezeigt, sondern sie kann auch unkontrolliert weitergegeben werden. Bei einer Gruppenplanung auf WhatsApp oder Facebook wäre es von Vorteil, zusätzlich eine Verbindungsperson zu benennen, die Freunde ohne dortige Anbindung benachrichtigen könnte. Konsequent wäre jedoch ein vollständiger Verzicht auf Apps, die auf Kontakte im Handy bzw. dem Telefonbuch zurückgreifen und die Daten mit den eigenen Beständen abgleichen können.

Laden Sie Ihr Adressbuch nicht in einen Kommunikationsdienst hoch. Denn die Daten Ihres sozialen Umfeldes werden damit ebenfalls übertragen.

Wen erfasst die Kamera Ihres Handys? Überkleben Sie gegebenenfalls die beiden Kameralinsen auf Ihrem Handy.

MEDIENKOMPETENZ

PASSWÖRTER

Bei vielen Aktivitäten im Web benötigen Sie digitale Konten, sogenannte Accounts, um einen Zugang zu erhalten. Konten sind ein zentraler Bereich, wenn es um Ihre Sicherheit geht, denn sie können von Fremden übernommen bzw. gehackt werden, um Ihre Identität zu beschädigen oder Bestellungen auf Ihrem Namen vorzunehmen.

Es wird häufig unterschätzt, wie wichtig Passwortsicherheit ist. Da es sehr bequem ist, einfach dasselbe Passwort für alles Mögliche zu nutzen, sind unsichere Passwörter noch immer einer der Hauptgründe für übernommene Accounts. Es ist wichtig, dass Sie mit sicheren Passwörtern arbeiten. Diese setzen sich wie folgt zusammen:

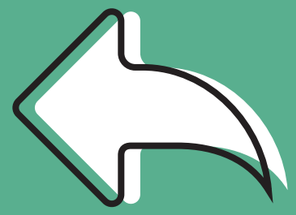
_SO*NDER/ZEICHEN!

Mindestens

12

ZEICHEN

Keine Worte, Namen, Geburtsdaten



Klein- und GROSSBUCHSTABEN

0100
1101
0110

ZIFFERN

WAS KÖNNEN SIE TUN?

Benutzen Sie verschiedene Passwörter für Ihre Accounts. Verwenden Sie einen Passwortmanager, um Ihre Passwörter abzuspeichern.

Es gibt Eselsbrücken, die es einem einfacher machen, sich Passwörter zu merken:
Eine Eselsbrücke durch einen längeren Satz zu bilden und die Anfangsbuchstaben der Wörter als Passwort zu nutzen, ist eine einfache Methode, um ein sicheres Passwort zu bilden. Zudem lässt es sich einfach merken. Zum Beispiel: „Das FRIEDA Frauenzentrum setzt sich für die Rechte von Frauen* ein!“ = DFFssfdRvF*e! Zusätzlich kann man dann noch einzelne Buchstaben durch Zahlen ersetzen, D=0, F=7, S=5, z.B: 07755Rv7*e!

Wählen Sie für Ihre Passwörter niemals einfache Begriffe wie etwa Namen (z.B. vom Haustier), Geburtstage, schlichte einzelne Wörter wie "passwort" oder "hallo" oder häufige Zeichenketten oder Zahlenreihen, wie z.B. "123456789".

Wählen Sie kein zu kurzes Passwort. Je kürzer das Passwort, desto leichter lässt es sich erraten.

Verschicken Sie Passwörter niemals unverschlüsselt per E-Mail. Bringen Sie Ihre Passwörter nicht auf Post-its z.B. am Monitor an. Und auch die Unterseite der Tastatur ist kein sicherer Ort. Ihre Passwörter sind vertraulich und nur für Sie bestimmt. Passwörter, die zuvor in der Partnerschaft geteilt wurden, sind im Falle von Cyberstalking leicht einsetzbar. Es empfiehlt sich daher, Passwörter spätestens nach der Trennung zu ersetzen.

Und zu guter Letzt: Auch beim Umgang mit Passwörtern können Sie ein gutes Vorbild sein. Nicht nur, indem Sie die oben genannten Punkte berücksichtigen und mit anderen darüber sprechen. Sondern auch, indem Sie deutlich sichtbar wegsehen, wenn jemand ein Passwort eingibt. Das dient nicht nur Ihrem Selbstschutz, um nicht in Verdacht fremder Passwortnutzung kommen zu können, sondern gilt in Computerkreisen mittlerweile als Sache der Höflichkeit.

FAKES

Auf Facebook und anderen Plattformen werden viele Informationen geteilt, deren Wahrheitsgehalt oft ungeklärt ist. Zu schnell kann durch einen ReTweet, das "Teilen" oder das Weiterleiten von E-Mails zu deren Verbreitung beigetragen werden.

WAS KÖNNEN SIE TUN?

- Hinterfragen Sie Informationen grundsätzlich und teilen Sie nur solche, von deren Authentizität Sie sich überzeugt haben. Beachten Sie bei der Weitergabe auch etwaige Urheberrechte.
- Teilen Sie Grafiken aufgearbeiteter Daten nur, wenn sie mit einer Quellenangabe versehen sind.
- Benennen Sie immer Ihre Quellen.
- Machen Sie Meinungen oder Vermutungen als solche kenntlich.

E-MAIL

Die E-Mail ist im Arbeitsalltag nicht mehr wegzudenken und auch privat ist sie noch eine der besten Formen, online zu kommunizieren. E-Mails kommen plattformunabhängig zum Einsatz und funktionieren auch bei unterschiedlichen Anbietern der Kommunikationspartner. Daher sollte E-Mail bevorzugt genutzt werden. Man zwingt damit niemanden, fragwürdige Nutzungsbestimmungen zu akzeptieren, um kommunizieren zu können. Doch auch hier gibt es einiges zu beachten.

WAS KÖNNEN SIE TUN?

- Achten Sie auch hier besonders gut auf Ihr E-Mail-Passwort. Denn hat eine Person Zugriff auf Ihr Passwort, kann sie sich alle anderen Passwörter zuschicken lassen.
  Achtung: Sollten Sie eine Passwort-Vergessen-Mail erhalten, die Sie nicht bestellt haben, ändern Sie sofort Ihr Passwort. Es könnte ein Zeichen dafür sein, dass jemand Ihre Mails mitliest.

- Verwalten Sie Ihre Mails nicht im Browser, sondern laden Sie diese auf Ihren Computer herunter. Installieren Sie dafür ein Mailprogramm.

- Überlegen Sie, ob der Wechsel zu einem vertrauenswürdigen E-Mail-Anbieter mit Sitz in Deutschland oder Europa wegen der strengeren Datenschutzbestimmungen lohnt.

- Öffnen Sie nur Anhänge von Absendern, die Ihnen bekannt sind und selbst dann nur mit Bedacht. Manche E-Mails sehen aus wie Mahnschreiben und verweisen für genauere Informationen auf den Anhang. Lassen Sie sich nicht aufs Glatteis führen. Löschen Sie die Nachricht, ohne den Anhang zu öffnen.

- Wenn Sie eine E-Mail an mehrere Menschen schicken, überlegen Sie vorher, ob diese die Mailadressen der anderen mitgeteilt bekommen sollen. Anderenfalls nutzen Sie die "Blindcopy"-Funktion. Sie erkennen sie daran, dass im Adressfeld nicht "An" oder "CC" steht sondern "BCC". Mailadressen, die hier eingefügt werden, können von den anderen Empfängerinnen und Empfängern nicht gesehen werden.

- Wenn jemand Sie per E-Mail nach einer Mailadresse einer anderen Person fragt, geben Sie diese nicht einfach weiter. Schicken Sie stattdessen eine E-Mail an die anfragende Person und nehmen Sie die Person, deren Mailadresse erfragt wurde, im BCC-Feld auf. So ist diese informiert und kann bei Interesse selber aktiv werden.

- Verschlüsseln Sie Ihre Mails. Es ist zwar etwas kompliziert, aber die Mühe lohnt sich. Eine schrittweise Anleitung in einfacher Sprache bietet u.a. die Free Software Foundation Europe unter https://emailselfdefense.fsf.org/de/. Weitere Informationen zum Wie und Warum der E-Mail-Verschlüsselung finden Sie auch unter https://digitalcourage.de/digitale-selbstverteidgung/e-mails-verschluesseln-wird-immer-einfacher.

IDENTITÄTS-DIEBSTAHL

Da taucht plötzlich ein Facebook-Profil mit Ihrem Foto und Ihren Daten auf. Sie erhalten teure Pakete, die Sie nicht bestellt haben. Wer an Ihre Daten gelangt ist, kann sich als Sie ausgeben.
Unter Identitätsdiebstahl versteht man, dass jemand Ihre Identität nutzt, um einen Dienst zu nutzen oder um Sie gezielt anzugreifen. Ein Identitätsdiebstahl ist sehr leicht – Name, Geburtstag und Geburtsort genügen oft schon, um sich im Internet als eine andere Person auszugeben.

WAS KÖNNEN SIE TUN?

Geben Sie persönliche Daten wie Geburtstag und -ort nur dann heraus, wenn es wirklich notwendig ist und Sie der anfragenden Stelle vertrauen. Fragen Sie gegebenenfalls nach, weshalb und wofür diese Daten gebraucht werden.

Geben Sie Ihren Personalausweis nicht als Pfand heraus oder kopieren Sie ihn. Wollen Sie keinen Nachteil erleben, fragen Sie an, welche Informationen des Personalausweises benötigt werden und schwärzen Sie den Rest. Nach der Schwärzung noch einmal kopieren, da die Daten sonst oft noch erkennbar sind.

Bringen Sie jeden Fall von Identitätsdiebstahl zur Anzeige. Auch vermeintlich harmlose Fälle können ein Hinweis darauf sein, dass es noch schwerere Fälle gibt, die Ihnen nur noch nicht bekannt sind.

Sammeln Sie Beweise (Screenshots, ganze Seite speichern, Zeuginnen und Zeugen) und kümmern Sie sich danach selbst darum, dass möglichst schnell die gefälschten Seiten in den sozialen Medien gelöscht werden. Die Betreiber der jeweiligen Seiten helfen Ihnen hier gerne weiter.

FOTOS SPEICHERN

Machen Sie sich generell Gedanken um den Umgang mit Ihren Fotos. Und das nicht nur im Fall von Nacktfotos, die sicherlich einen besonderen Schutz verdienen.

WAS KÖNNEN SIE TUN?

Synchronisieren Sie Fotos nur in der Cloud, wenn Sie diese in den Einstellungen als „rein privat“ gekennzeichnet haben oder verzichten Sie ganz auf diese Form der Speicherung. Denn Sie fotografieren ja nicht nur sich selbst und es könnte Menschen geben, die damit nicht einverstanden sind.

Speichern Sie Fotos auf mindestens einer verschlüsselten Festplatte. Besser wären mehrere, die getrennt voneinander gelagert werden für den Fall, dass eine unbrauchbar wird.

Für Situationen, in denen Sie ganz sichergehen wollen, fotografieren Sie analog. Mit einer Sofortbild-Kamera müssen die Bilder nicht mal zum Entwickeln abgeben.

Bei Nacktaufnahmen können Sie nach der Bildübermittlung die sofortige Löschung vom Fotoapparat in Ihrem Beisein verlangen. Beachten Sie dabei, dass es Apparate gibt, die mehr als ein Speichermedium haben (z. B. im Gehäuse oder auf Karten).

MEDIENKOMPETENZ

WLAN-ZUGANG IM WEB UNTERWEGS

In der Regel wird der Internet-Zugang über einen Router hergestellt. Im Router wird auch der WLAN-Zugang eingerichtet und mit einem Verschlüsselungsverfahren und einem Passwort gesichert. Mit mobilen Geräten nutzen wir aber nicht nur das eigene heimische WLAN, sondern auch öffentliche Hotspots oder Access Points (so werden WLAN-Zugänge in öffentlichen Netzwerken genannt). Viele unserer mobilen Geräte speichern diese Zugangsdaten, wenn sie einmal erfolgreich eingerichtet sind. Dann werden diese Verbindungen automatisch hergestellt, wenn das mobile Gerät in der Nähe des Hotspots ist. Das ist zwar praktisch, birgt aber auch Sicherheitsrisiken.

WAS KÖNNEN SIE TUN?

Schalten Sie die WLAN-Funktion nur dann ein, wenn Sie sie benötigen! Ein abgeschaltetes WLAN bietet keine Angriffsfläche.

Rufen Sie vertrauliche Daten und E-Mails nur über WLAN-Netze ab, denen Sie vertrauen. Vorsicht bei fremden WLAN-Netzen/Hotspots sowie bei öffentlichen WLAN-Netzen in Hotels, auf Flughäfen usw.

Eventuell ist Ihr Smartphone oder Ihr Notebook in einem öffentlichen Netzwerk sichtbar für Andere. Schützen Sie daher Ihre Daten vor fremden Blicken.

In den Einstellungen Ihres Gerätes sollten Sie die automatische Anmeldung an Hotspots deaktivieren.

BROWSER

Browser sind Programme, die wir nutzen, um Webseiten aufzurufen. Internet Explorer, Edge, Mozilla Firefox oder Google Chrome sind Beispiele dafür. Neueste Versionen und regelmäßige Updates tragen erheblich zu Ihrer Sicherheit bei. Zudem sollten Sie sichere Nutzungsmöglichkeiten und Systemeinstellungen in Ihrem Browser kennen und benutzen.

SUCHMASCHINEN

Suchmaschinen sind für die Nutzung des Internets hilfreich. Sie haben eine sehr wichtige Funktion, weshalb es ratsam ist, sich die genutzte Suchmaschine genauer anzusehen. Einige Suchmaschinen stehen in dem Verdacht, umfassende Daten über Sie zu sammeln, diese zu verknüpfen und zu verkaufen.

WAS KÖNNEN SIE TUN?

Suchen Sie sich eine Suchmaschine aus, die Ihren Ansprüchen entspricht. Erkundigen Sie sich, welche Anbieter es gibt.

Ändern Sie ihre Standard-Suchmaschine in Ihrem Browser. Gehen Sie dazu in die Einstellungen Ihres Browsers und stellen Sie unter "Suche" die Suchmaschine Ihrer Wahl ein. Browser sind etwas unterschiedlich. Falls es keinen Unterpunkt "Suche" gibt, finden Sie die Einstellung sicherlich an einem anderen Ort in den Einstellungen.

SURFEN

Beim Surfen im Internet hinterlassen Sie besonders viele Spuren. Daher ist es lohnenswert, sich auch hier kritisch mit den eigenen Gewohnheiten auseinanderzusetzen und etwas Zeit in die Einstellung des Browsers zu investieren.

WAS KÖNNEN SIE TUN?

Installieren Sie einen Werbeblocker in Ihrem Browser. Denn Werbung kann nicht nur störend sein, sie kann Sie auch ausspionieren. Manche Internetseiten verlangen, den Werbeblocker zu deaktivieren. Machen Sie sich klar, dass diese damit nicht nur fordern, dass Sie das "Keine Werbung!"-Schild an Ihrem Briefkasten entfernen, sondern dass Sie auch noch die Haustüre unverschlossen halten sollen.

Vertrauen ist eine wichtige Frage beim Surfen. Um Ihnen die Frage nach sicheren, vertrauenswürdigen Webseiten zu erleichtern, gibt es sogenannte Zertifikate, die mittlerweile die meisten Internetseiten nutzen. Sollte solch ein Zertifikat fehlen oder abgelaufen sein, erhalten Sie in Ihrem Browser eine Warnung, wenn Sie sich auf dieser Seite befinden.

Achten Sie darauf, dass in der Adresszeile einer Website (also dort, wo sie das www.xyz.de eingeben) hinter dem "http" immer ein "s" steht. Das Kürzel "https" zeigt Ihnen an, dass die aktuelle Verbindung verschlüsselt ist. Geben Sie deshalb nirgendwo ein Passwort ein, wo nur "http" steht. Beim Besuch einer sicheren Webseite wird in der Adressleiste zudem ein Sperrschloss/Schloss-Symbol angezeigt.

Denken Sie immer daran, sich auszuloggen, wenn Sie einen Dienst nicht mehr brauchen. Schließen Sie das Fenster nach jeder Benutzung. Das gilt besonders für öffentlich zugängliche Computer, z. B. in Internetcafés.

Löschen Sie regelmäßig Ihren Browserverlauf oder überlegen Sie sich, ob Sie diesen überhaupt speichern wollen. Auch dies lässt sich in den Einstellungen Ihres Browsers einstellen. Richten Sie für Gäste, die Ihren PC benutzen, ein extra Gastkonto mit eingeschränkten Rechten ein.

SMARTPHONE UND APPS

Die meisten Menschen verfügen heute über ein Smartphone. Übertragen auch Sie diesem kleinen Taschencomputer mehr und mehr Aufgaben? Dann ist es vielleicht auch für Sie an der Zeit, sich diese Geräte einmal genauer anzusehen.

WAS KÖNNEN SIE TUN?

Mit Ihrer Wahl für ein bestimmtes Smartphone entscheiden Sie sich automatisch für ein Betriebssystem wie beispielsweise Android oder iOS mit. Damit verbunden ist in der Regel eine Plattform – meist store genannt – über die Sie passende Apps für Ihr Smartphone beziehen können. Voraussetzung ist immer ein Account, sprich eine Anmeldung bei dem Anbieter wie Google Playstore für Android bzw. Apple Appstore für iOS.

Prüfen Sie, welche Apps Sie tatsächlich benötigen. Je weniger Programme und Apps installiert sind, desto kleiner ist die Angriffsfläche für das gesamte System. Deinstallieren Sie alle Apps, die Sie nicht (mehr) benötigen.

Installieren Sie nur Apps aus zuverlässigen Quellen.

Verweigern Sie den installierten Apps Zugriff auf Daten, die diese nicht brauchen. Warum möchte die Taschenlampen-App Zugriff auf Ihr Adressbuch?

Sie haben oben bereits einiges über Accounts, E-Mails und Passwörter gelesen – das alles bündeln Sie nun in einem kleinen Smartphone. Dazu kommen Fotos und ggf. andere Daten, die Sie ebenfalls auf Ihrem Smartphone speichern. Das sind viele gute Gründe, um dieses nicht aus den Augen zu lassen und zu sichern.

Belegen Sie Ihr Smartphone über die Einstellungen in Ihrem Betriebssystem mit einem Entsperrungscode. Wählen Sie dazu eine mindestens 6-stellige Zahl, bei der einige Zahlen mehrfach vorkommen (aber nicht ausschließlich!). Vorsicht bei der Nutzung eines gewischten Zeichens als Entsperrungscode, denn dies ist erkennbar, wenn das Handy schräg gegen das Licht gehalten wird.

Pärchen-Apps werden nicht ohne Grund auch „Stalker-Apps“ genannt. Was romantisch von den Anbietern beworben wird, kann sich im Falle einer übergriffig werdenden Beziehungsform gegen Sie wenden. Denn viele dieser Apps teilen auch den aktuellen Standort mit.

MEDIENKOMPETENZ

CLOUD

Zugegeben: Es ist bequem, Cloud-Dienste zu nutzen. Gerade wer sich nicht gut auskennt, findet hier vermeintlich eine einfache Lösung. Doch die wolkige Cloud gibt es eigentlich gar nicht. Es handelt sich um ganz „normale“ Computer (mit unvorstellbar umfangreichen Speichern). Überlegen Sie sich, ob Sie Ihre Daten und Fotos den Computern fremder Menschen anvertrauen wollen. Oder verschlüsseln Sie Ihre Daten, bevor Sie sie in die Cloud hochladen.

FESTPLATTEN VERSCHLÜSSELN UND DATENSICHERUNG

Es gibt einen wichtigen Unterschied zwischen Datenschutz und Datensicherheit. Beides ist jedoch wichtig. Datenschutz bedeutet, dass niemand unbefugt Informationen über Sie erhält. Datensicherheit bedeutet, dass Ihnen Ihre eigenen Daten (wie Fotos, Textdateien usw.) nicht abhanden kommen. Es ist daher sehr wichtig, die eigenen Daten regelmäßig extern zu sichern wie zum Beispiel durch regelmäßige Backups. Mit der externen Speicherung haben Sie Ihre Daten gesichert. Um sie aber darüber hinaus auch zu schützen, sollten Sie diese auf verschlüsselten Datenträgern ablegen.

WAS KÖNNEN SIE TUN?

Wie Sie Ihr Smartphone oder Ihren Computer verschlüsseln hängt vom Betriebssystem ab.

Achtung! Beachten Sie bitte, dass verschlüsselte Speichermedien z.B. durch ein Passwort oder ein entsprechendes Programm geschützt werden. Wenn Sie dieses verlieren, könnte es passieren, dass Sie sich selbst von Ihren Daten "aussperren". Gehen Sie daher bei der Verschlüsselung mit Umsicht vor und holen Sie sich im Zweifelsfall Unterstützung.

Legen Sie regelmäßig Sicherheitskopien auf einer - verschlüsselten - externen Festplatte an und bewahren sie an einem separaten Ort auf.

Es gibt in Elektronikfachgeschäften fertig konfigurierte Festplatten, mit denen es sehr einfach ist, die Daten auf der eigenen Festplatte zu sichern. Erkundigen Sie sich vor dem Kauf, ob diese verschlüsselt sind und Ihren Ansprüchen genügen.

SICHERHEITSSOFTWARE UND UPDATES

Zu guter Letzt noch Hinweise zu erforderlichen Sicherheitsmaßnahmen für Hard- und Software.

WAS KÖNNEN SIE TUN?

Jede Hardware benötigt aktuelle Schutzprogramme. Es gibt diese auch kostenlos im Internet. Ein solches Programm sollten Sie als Mindestschutz installieren.

Jedes veraltete Programm stellt ein Sicherheitsrisiko dar. Sie sollten daher stets Ihr Betriebssystem, Ihren Browser, Ihre Anwendungsprogramme und Ihre Apps auf dem neuesten Stand halten. Lassen Sie die Updates automatisch installieren. Nur so werden neu erkannte Sicherheitslücken geschlossen. Updates „wegdrücken“, weil es gerade nicht passt oder weil Sie die Notwendigkeit noch nicht sehen, ist für Ihre Sicherheit im Netz grob fahrlässig.