Verwaltung
im Verein

digital verein(t)

Sicher im Netz:
Passwörter, Suchmaschinen und WLAN

Impressum

Herausgeber:
Landesarbeitsgemeinschaft der Freiwilligenagenturen/-Zentren und Koordinierungszentren Bürgerschaftlichen Engagements in Bayern (lagfa bayern e.V.)
Projekt: digital verein(t)

Geschäftsführung:
Beatrix Hertle
Schaezlerstraße 13 1/2
86150 Augsburg
+49 (0) 821 207148 10
www.lagfa-bayern.de

2. Auflage 2024

Redaktion:
Dr. Elisabeth Maria Hofmann,
Daniel Helmes (BBE), Petra Rollfing

Lektorat:
Leonore Lukschy, Sebastian Honert

Gestaltung und Satz:
freistil grafik&design, München

Projektpartner:
Deutschland sicher im Netz e.V. (DsiN)

Projektleitung:
Joachim Schulte (DsiN)

digital verein(t) ist eine Initiative des Bayerischen Staatsministeriums für Digitales und hilft ehrenamtlich engagierten Menschen und Vereinen, die Chancen der Digitalisierung zu nutzen: mit Handbüchern, Workshops, Online-Seminaren sowie einem mobilen Ratgeberteam. Konzipiert, koordiniert und stetig weiter entwickelt wird digital verein(t) durch die lagfa bayern e.V. – Landesarbeitsgemeinschaft der Freiwilligenagenturen – in Zusammenarbeit mit Deutschland sicher im Netz e.V. (DsiN).

Dieses Handbuch berücksichtigt die Grundlagen der „Cyberfibel – Für Wissensvermittler:innen in der digitalen Aufklärungsarbeit“, ein Angebot von Deutschland sicher im Netz e.V. (DsiN) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefördert durch

Bayerisches Staatsministerium für Digitales

Ein Projekt von

lagfa bayern

In Zusammenarbeit mit

DsiN Deutschland sicher im Netz

Sicher im Netz: Passwörter, Suchmaschinen und WLAN

Handbuch von digital verein(t)

Die fünf Themenbereiche von digital verein(t) kommen direkt aus der Praxis des freiwilligen Engagements. Mit den digital verein(t)-Handbüchern zu den Themen „Öffentlichkeitsarbeit im Verein“, „Verwaltung im Verein“, „Zusammenarbeit im Verein“, „Finanzen im Verein“ und „Digitale Trends im Verein“ macht sich Ihr Verein fit fürs Netz.

© StmD, Andreas Gebert

Dr. Fabian Mehring
MdL, Bayerischer
Staatsminister
für Digitales

Liebe Leserinnen, liebe Leser,

die besondere Lebensqualität in unserer Heimat lebt von unserem bayerischen Vereinswesen und vom bürgerlichen Engagement der Menschen im Freistaat – von Menschen wie Ihnen, die darum wissen und deshalb stets mehr tun als nur ihre Pflicht! Damit Sie sich auch in Zukunft mit vollem Herzblut Ihren eigentlichen Aufgaben und Zielen widmen können, unterstützen wir mit digital verein(t) bayernweit die Digitalisierung in den Vereinen auch in der zweiten Förderlaufzeit bis 2026. Auf diese Weise bringen wir Heimat und Zukunft zusammen und bahnen dem Ehrenamt seinen Weg in die digitale Welt!

Diese Handbuchreihe mit praxisnahen Informationen soll den Weg zum sicheren und souveränen Handeln im World Wide Web ebnen, damit unsere Vereine von den technologischen Entwicklungen profitieren. Wenn die Digitalisierung Einzug in den Vereinsalltag hält, können sich Organisationen nachhaltig und zukunftsorientiert aufstellen und Ressourcen noch effizienter nutzen. Um den Prozess hin zum digitalen Verein zu vereinfachen, ist die Vernetzung der Organisationen und Initiativen sowie der Austausch von Erfahrungen untereinander gewinnbringend.

Wissen teilen und voneinander profitieren, wird auch in diesem Kooperationsprojekt gelebt: Die „Landesarbeitsgemeinschaft der Freiwilligenagenturen in Bayern (lagfa bayern)“ setzt das Projekt mit mittlerweile 28 eingerichteten lokalen Kompetenzstandorten und mit mehreren großen Landesverbänden aus dem Ehrenamt um. So werden Sie und Ihr Verein beim digitalen Wandel gut begleitet. Mit „Deutschland sicher im Netz“ ist auch weiterhin ein wichtiger Partner mit im Boot, um die Lehrmaterialien stets weiterzuentwickeln.

Ich wünsche Ihnen viel Vergnügen bei der Lektüre und bedanke mich von Herzen für Ihr Engagement!

Ihr

Gefördert durch
Bayerisches Staatsministerium
für Digitales

Inhalt

Über dieses Handbuch

Wenn der Schwimmverein ins Trockene bittet und bei seiner Mitgliederversammlung eine drahtlose Internetverbindung (WLAN) zur Verfügung stellt, sind nur wenige Vorkehrungen nötig, um das Netz sicher zu nutzen. So können Mitglieder und ihre Geräte genauso geschützt werden wie der Vereinsrechner, der möglicherweise über dasselbe Netzwerk im Internet ist und zugleich den Datenschatz des Vereins beherbergt. Aber auch bei Kleinigkeiten im Vereinsalltag helfen ein paar Tipps, nicht unnötig sensible Daten einzelner Mitglieder in Umlauf zu bringen. Wie kann beispielsweise ein Mitglied im Basketballverein anderen sicher mitteilen, dass die Kursleitung krank ist und das Training kurzfristig abgesagt werden muss?

digital verein(t) hat **16 Tipps** formuliert, die helfen, die digitalen Chancen sicher in der Vereinswelt zu nutzen. Im ersten Kapitel geht es darum, wie Computer, Tablets oder Smartphones und Anwendungen sicher eingerichtet werden. Das zweite Kapitel erläutert, wie das Surfen im Internet sicher gelingt, ohne zu viele Informationen von sich preiszugeben. Und schließlich zeigt das dritte Kapitel, wie persönliche Daten geschützt werden können.

In den digital verein(t)-Kästen befinden sich kurze und praktische Hilfsmittel:

Informieren

Hier werden Fachbegriffe verständlich erklärt.

Machen

Hier werden digitale Werkzeuge vorgestellt, welche sofort verwendet werden können.*

Üben

Hier gibt es Übungsaufgaben, um das neue Wissen anzuwenden.

Weiterlesen

Hier werden Websites und digital verein(t)-Handbücher mit weiterführenden Informationen empfohlen.

* Die ausgewählten Werkzeuge sind bevorzugt frei zugänglich und zumindest in der Basisversion unentgeltlich. Sie arbeiten außerdem datensparsam, transparent und möglichst werbefrei. Die Aufzählung verschiedener Alternativen folgt keiner Rangfolge, sondern ist alphabetisch geordnet.

1 Passwörter & Firewall

1

Passwörter & Firewall: Geräte absichern

Wo Menschen zusammenkommen, um gemeinsam im Verein zu arbeiten und sich auszutauschen, entstehen schnell große Datenmengen. Warum ist Datensparsamkeit wichtig? Wie gelingt es, sich ein sicheres Passwort zu merken? Und mit welcher Software können Geräte geschützt werden? Um Geräte richtig zu bedienen und notwendige Sicherheitseinstellungen vorzunehmen, muss niemand Expert:in für technische Fragen sein. digital verein(t) zeigt in diesem Kapitel, wie es geht.

Tipp 1 / **Mit den eigenen Daten und Daten anderer sparsam umgehen.**

Datensparsamkeit ist eine grundsätzliche Verhaltensregel im Internet. Um personenbezogene und sensible Daten zu schützen, sollten immer nur so viele Daten angegeben werden, wie es für die jeweilige Anwendung unbedingt notwendig ist.

i

Personenbezogen sind alle Daten, die eine natürliche Person identifizierbar machen. Dazu gehören unter anderem Name, Adresse, Geburtsdatum, aber auch Fotos und Fingerabdrücke (biometrische Daten) sowie Kontodaten und Kfz-Kennzeichen. Besonders sparsam sollte mit sensiblen Daten umgegangen werden, die als besonders schützenswert gelten. Dazu zählen beispielsweise die ethnische Herkunft, politische und religiöse Überzeugungen sowie genetische und biometrische Daten.

Grundsätzlich ist beim Surfen im Internet immer abzuwägen, bei welcher Gelegenheit personenbezogene Daten preisgegeben werden. Das gilt nicht nur für die eigenen, sondern auch für die Daten von Vereinskolleg:innen. Die folgenden Grundregeln helfen beim alltäglichen Datenschutz:

- Beim Versand von **Rund-E-Mails** sollte das Adressfeld „Blindkopie“ (BCC) verwendet werden. Dadurch können die Empfänger:innen die Adressen der anderen nicht sehen. Insbesondere dann, wenn sich einige der Empfänger:innen nicht kennen, sind große offene E-Mail-Verteiler sogar verboten und können Bußgelder nach sich ziehen.

- Bei der **Nutzung von Apps** sollte darauf geachtet werden, dass diese nicht auf alle Smartphone-Funktionen zugreifen können. So ist beispielsweise bei einer Nachrichten-App der Standort nicht relevant und eine Navigations-App benötigt keinen Zugriff auf die Freundesliste. Welche Daten ein Dienst oder eine App erhebt, speichert und wie sie verwendet werden, steht in den Datenschutzerklärungen der Anbieter. Die Berechtigungen können unter den App-Einstellungen jederzeit angepasst werden.

- Es sollte vermieden werden, sich für Internetdienste über **Social-Media-Konten** anzumelden. Dadurch kann das Kontaktnetzwerk ausgelesen werden.

- Möglichst nicht mit dem eigenen Klarnamen (das ist der bürgerliche Vor- oder Nachname) bei **Internetdiensten** anmelden. Es sollten außerdem nur Daten angegeben werden, die als „Pflichtfeld“ gekennzeichnet sind.

- Unbedingt mit Bedacht entscheiden, welche **Bilder** online zur Verfügung stehen. Denn auch Fotos und Videos enthalten persönliche Informationen. Beispielsweise kann mit einem veröffentlichten Foto vom Vereinsausflug mitgeteilt werden, dass das Vereinsheim gerade leer steht.

- Die **Bluetooth- und NFC-Funktion** sollte ausgeschaltet werden, wenn diese nicht benötigt wird, damit andere keinen Zugang zum Gerät erhalten können.

Tipp 2 / **Sichere Passwörter aus Buchstaben, Zahlen und Sonderzeichen erstellen.**

Egal, ob mit dem PC, Tablet oder Smartphone im Internet gesurft wird: Grundlegend dabei sind immer sichere Passwörter, aktuelle Software und ein aktuelles Anti-Viren-Programm. Passwörter schützen vor unerlaubten Zugriffen auf Programme und Geräte. Wer das Internet regelmäßig nutzt, braucht viele Passwörter, unter anderem für den Zugriff auf den Computer, für E-Mail-Programme, Profile in sozialen Netzwerken, Onlinebanking und für Kundenprofile in Onlineshops.

Es gibt sehr einfach zu merkende Passwörter wie zum Beispiel das eigene Geburtsdatum oder die Telefonnummer. Diese sind leider auch sehr unsicher. Ein sicheres Passwort hingegen kann von Angriffsprogrammen nicht so leicht geknackt werden. Ein paar einfache Tricks helfen, ein sicheres Passwort zu erstellen:

1. Je länger ein Passwort ist, desto sicherer ist es auch. Ein Passwort sollte aus mindestens acht Zeichen bestehen. Für das WLAN-Kennwort werden sogar 20 empfohlen.

2. Im Passwort sollten Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen vorkommen.

3. Im Passwort sollten keine persönlichen Daten wie Namen, Geburtsdatum oder Telefonnummer verwendet werden.

4. Für das Passwort keine Wörter aus dem Wörterbuch oder gängige Wiederholungs- und Tastaturmuster wie zum Beispiel asdfg, abcd oder 1234 benutzen. Im besten Fall sollte das Passwort keinen erkennbaren Sinn ergeben.

Um das Passwort zu schützen, sollte es nicht im Gerät abgespeichert werden. Das Passwort sollte auch nicht dort aufgeschrieben werden, wo es leicht auffindbar ist wie beispielsweise am Bildschirmmonitor oder im Kalender. Es ist jedoch in Ordnung, wenn das Passwort aufgeschrieben, in einen Briefumschlag gelegt und an einem sicheren Ort zuhause aufbewahrt wird. Außerdem gibt es hilfreiche Methoden, mit denen Passwörter sich im Alltag leichter merken lassen.

Die Merksatz-Methode

Eine bestimmte Aneinanderreihung von Zeichen, Buchstaben und Zahlen ergibt einen versteckten Sinn, wenn sie sich nur der Person erschließt, die das Passwort wissen darf. Mit der Merksatz-Methode kann solch ein sicheres Passwort erstellt werden, das alle Sicherheitsregeln erfüllt und dennoch einfach zu merken ist. Das funktioniert so:

1. Ein Satz mit mindestens acht Wörtern ausdenken, in dem auch Zahlen vorkommen. Für die Wörter „ein“ bzw. „eine“ kann auch die Zahl „1“ verwendet werden.

2. Nun alle Anfangsbuchstaben der Wörter nebeneinander aufschreiben. Wichtig ist, dass Groß- und Kleinschreibung beibehalten werden.

3. Am Ende auch das Satzzeichen aufschreiben. Fertig!

Ein Beispiel:

Persönlicher Satz: „Vor 10 Jahren haben wir 1 großen Pokal gewonnen!“ Anfangsbuchstaben, Zahlen und Satzzeichen nebeneinander (hier fett markiert): **V**or **10 J**ahren **h**aben **w**ir **1 g**roßen **P**okal **g**ewonnen**!**
Das Passwort lautet also: **V10Jhw1gPg!**

Dieses Passwort besteht aus mehr als acht Zeichen, aus Groß- und Kleinbuchstaben und enthält auch Sonderzeichen. Zwar steht es in Zusammenhang mit einem wichtigen Ereignis der Vereinsgeschichte, so dass es sich leicht merken lässt. Dieser Zusammenhang ist aber anderen Personen nicht ersichtlich, ganz im Gegensatz zu der Telefonnummer oder dem Geburtsdatum.

Zur Übung: Mit der Merksatz-Methode ein sicheres Passwort bilden. Dafür als Übung spielerisch mehrere Sätze ausprobieren und versuchen sich eins der Passwörter für ein paar Tage zu merken. Wenn dies gut klappt, kann das Passwort sicher verwendet werden, ohne dass es notiert werden muss.

Die Passwortkarte

Eine weitere Merkhilfe ist die Passwortkarte von Deutschland sicher im Netz e.V. Die Passwortkarte wird auf die folgende Weise verwendet:

Abbildung Passwortkarte

1. Im Koordinatensystem einen beliebigen Startpunkt auswählen.
2. Vom Startpunkt aus einen „Weg" in eine beliebige Richtung nehmen. Dabei ist die Verwendung von horizontalen, vertikalen, diagonalen Richtungen sowie auch von Richtungswechseln und Zickzack möglich. Die Länge des Weges sollte mindestens aus acht Zeichen bestehen.
3. Die Passworterstellung variiert, indem zum Beispiel die Zeichenfolge des Weges durch das Auslassen von Zeichen nach einem festen Muster verlängert wird. So kann auch eine enthaltene Zahl ausgeschrieben oder jeweils der erste und letzte Buchstabe vertauscht werden.
4. Merken muss man sich nur noch den Startpunkt und den Richtungsverlauf des Weges für das Passwort im Koordinatensystem. Fertig ist das sichere Passwort!

Tipp 3 / **Für jede Anwendung ein anderes sicheres Passwort verwenden.**

Es scheint auf den ersten Blick praktisch zu sein, ein komplexes Passwort gleich für alle Anwendungen zu verwenden. Das ist aber ein Fehler. Denn sollte einmal das Passwort geknackt werden, sind mit einem Schlag alle Anwendungen und Geräte unsicher. Hat sich beispielsweise jemand Zugang zum persönlichen E-Mail-Konto oder dem WLAN des Vereins verschafft, weiß diese Person auch das Passwort für das Bankkonto oder für die Konten in den sozialen Netzwerken. Daher sollte jede Anwendung mit einem eigenen Passwort geschützt werden.

Passwort-Manager

Bei einer großen Anzahl von Passwörtern ist es nicht leicht, einen Überblick zu behalten und sich alle Passwörter zu merken. Bei der Verwaltung der verschiedenen Passwörter im Verein können sogenannte Passwort-Manager helfen. Ein Passwort-Manager speichert nicht nur die ganzen Passwörter, sondern kann auch sichere Passwörter erstellen. Das Programm wird durch ein Hauptpasswort, ein sogenanntes Master-Passwort, für den Zugang geschützt. Mit diesem erfolgt der Zugriff auf alle anderen Passwörter.

Mit dem kostenlosen und quelloffenen Passwort-Management-Tool **KeePassXC** können Passwörter sicher erstellt, gespeichert und verwaltet werden. Die Passwörter werden in einer verschlüsselten Datenbank gespeichert, die durch ein Master-Passwort oder einen Hardware-Schlüssel gesichert ist. KeePassXC unterstützt verschiedene Betriebssysteme (Windows, macOS, Linux) und erlaubt das Importieren und Exportieren von Passwortdatenbanken in verschiedenen Formaten. Dank seiner Offline-Funktionalität bietet es große Datensicherheit ohne Cloud-Abhängigkeit.
keepassxc.org

Auch **Bitwarden** eignet sich für die sichere Verwaltung von Passwörtern. In der kostenfreien Version für private Nutzer:innen lassen sich unbegrenzt viele Passwörter sicher speichern. Auch hier wird die Zwei-Faktor-Authentifizierung eingesetzt, um das Konto doppelt vor unbefugten Zugriffen zu schützen. Elemente im Bitwarden-Konto können in der kostenlosen Variante ebenfalls mit anderen Nutzer:innen geteilt werden.
bitwarden.com/de-de/products/personal/

Im Internet und in Ratgebern ist häufig noch die Empfehlung zu finden, dass Passwörter regelmäßig zu ändern sind. Studien haben aber gezeigt, dass bei häufigen Passwortänderungen meistens schwächere Passwörter vergeben oder die bestehenden Passwörter nur geringfügig geändert werden. Beides wirkt sich negativ auf die Sicherheit der Passwörter aus. Allerdings sollte schnellstmöglich das Passwort geändert werden, wenn bekannt wird, dass der Internetanbieter Opfer einer Cyberattacke geworden ist.

Neben starken Passwörtern als ersten Faktor ist es sehr ratsam, Benutzerkonten durch einen zweiten Faktor zu schützen. Das kann eine Hardware-Komponente wie ein spezieller USB-Stick sein, eine vom Anbieter versendete SMS oder eine Authenticator App. Dieses Verfahren, bei dem die Anmeldung in zwei Schritten erfolgt, heißt Zwei-Faktor-Authentisierung (2FA).

Eine Möglichkeit zu überprüfen, ob die eigene E-Mail-Adresse von einem Cyberangriff betroffen ist, bietet der Identity Leak Checker vom Hasso-Plattner-Institut. Dieser gleicht die E-Mail-Adresse mit bekannten Cyberangriffen ab.
sec.hpi.de/ilc/

Ausführlichere Informationen zur Zwei-Faktor-Authentisierung mit konkreten Anwendungstipps bei sozialen Netzwerken und beim Online-Banking sind in den digital verein(t)-Handbüchern „Soziale Netzwerke kennenlernen: erste Schritte und Sicherheit“ und „Finanzen im Netz: Gelder verwalten, online einkaufen und bezahlen“ zu finden.

Tipp 4 / Geräte mit einem Anti-Viren-Programm und einer Firewall vor Schadsoftware schützen.

Vor dem Online-Start sollte auf jedem Gerät, mit dem der Verein im Internet agiert, ein aktuelles Anti-Viren-Programm und eine Firewall eingerichtet werden. Ein Anti-Viren-Programm schützt das Betriebssystem vor schädlicher Software aus dem Internet, stärkt also sein „Immunsystem“. Bereits beim Kauf sollte darauf geachtet werden, dass ein aktuelles Anti-Viren-Programm auf dem Computer, Laptop, Smartphone oder Tablet vorinstalliert ist. Eine Firewall (auf Deutsch: Brandmauer) gehört zur Grundausstattung internetfähiger Geräte und sollte ebenfalls schon vorinstalliert sein. Ihre Funktion lässt sich mit einem Türsteher vergleichen: Sie verhindert, dass ungebetene Gäste ins Haus gelangen und sich dort umschauen, Sachen mitnehmen oder gar zerstören.

Computerviren sind Programme, die sich in andere Computerprogramme einschleusen, zum Beispiel durch das Öffnen von E-Mail-Anhängen unbekannter Absender:innen. Einmal gestartet, können Viren Veränderungen am Computersystem auslösen und den Computer kaputt machen. Der eigene Computer kann auch andere Geräte anstecken, beispielsweise durch Datenübertragung zwischen zwei Computern.

Für einen soliden Schutz des Betriebsprogramms sind kostenlose Anti-Viren-Programme ausreichend. Wir stellen die drei gängigsten vor:

Die Anti-Viren-Software **avast! Free Antivirus** scannt das Betriebssystem auf Sicherheits- und Leistungsprobleme und informiert, wie die Probleme zu beheben sind. Die Zusatzfunktion „WLAN-Inspektor" erkennt Schwachstellen im WLAN und warnt, wenn sich Unbefugte Zugang zum Netzwerk verschafft haben. Außerdem ist eine verhaltensbasierte Erkennung von Schadsoftware integriert, die sicherstellt, dass ungefährliche Anwendungen nicht plötzlich zur Gefahr werden.
www.avast.com/de-de/free-antivirus-download

AVG AntiVirus Free schützt vor Viren, dem Ausspähen persönlicher Daten sowie vor anderer Schadsoftware. Auch unsichere Links, Dateien und E-Mail-Anhänge werden von dem Programm blockiert. Für einen umfassenden Schutz werden etwaige Sicherheitsupdates in Echtzeit heruntergeladen.
www.avg.com/de-de/free-antivirus-download

Das Programm **Avira Free Antivirus** bietet neben einem umfassenden Schutz vor Schadsoftware einen Kinderschutz für soziale Netzwerke sowie einen Schutz gegen den Diebstahl persönlicher Daten. Außerdem ist das Programm in der Lage, beschädigte Dateien zu reparieren beziehungsweise wiederherzustellen.
www.avira.com/de/free-antivirus-windows

Zur Übung: Welches Anti-Viren-Programm ist auf den Geräten des Vereins installiert? Auf jedem Gerät den individuellen Schutz prüfen und wenn nötig aktualisieren.

Ist noch kein Anti-Viren-Programm und/oder keine Firewall auf dem Computer installiert, kann im Windows Defender Sicherheitscenter oder im App Store nach geeigneten Programmen gesucht werden. Eine weitere Möglichkeit ist, im Internet nach guten oder beliebten Programmen zu recherchieren. Etablierte Computerfachzeitschriften testen regelmäßig Anti-Viren-Programme und Firewalls. Auf ihren Websites kann nachgelesen werden, was unabhängige Expert:innen empfehlen.

Tipp 5 / Das Betriebssystem und die Software regelmäßig aktualisieren.

In regelmäßigen Abständen erscheinen auf Smartphones oder Computern Aufforderungen, Aktualisierungen, sogenannte **Updates** durchzuführen. Solche Updates schützen Geräte vor Hackern und Viren, da bei Betriebssystemen und Anwendungen regelmäßig Sicherheitslücken entdeckt werden. System- und Softwareupdates stopfen diese Löcher durch sogenannte Patches (auf Deutsch: Flicken). Werden diese Updates nicht ausgeführt, können Hacker die Sicherheitslücke mit entsprechend programmierter Schadsoftware ausnutzen. Darum ist es wichtig, dass die geforderten Updates immer zeitnah durchgeführt werden.

Auch Anti-Viren-Programme brauchen regelmäßige Updates. Die Programme sind in der Regel so konzipiert, dass sie automatisch und kostenlos aktualisiert werden (automatisches Update). Sie können jedoch auch manuell aktualisiert werden.

Bei Windows wird der Status der Anti-Viren-Software im **Windows Defender Sicherheitscenter** angezeigt. Im Start-Menü unter „Windows-Systemsteuerung“ zu finden und dann „Sicherheit und Wartung“ auswählen. Wenn Windows die Anti-Viren-Software erkennen kann, wird diese unter „Virenschutz“ aufgelistet. Falls die Software aktualisiert werden muss, auf „Jetzt aktualisieren“ klicken. Bei Apple-Computern ist der Aktualisierungsstatus im App Store zu finden. Für manuelle Aktualisierungen auf die angezeigten neu verfügbaren Updates klicken und dann die gewünschten Aktualisierungen einzeln oder insgesamt auswählen.

Wenn das Anti-Viren-Programm nicht im Sicherheitscenter des Geräts beziehungsweise im App Store angezeigt wird, ist es im Downloadbereich auf der Website des Programmherstellers zu finden. Dort kann nach dem Update für die Softwareversion im passenden Betriebssystem gesucht werden. Nach der Deinstallation der alten Version kann die neue Version einfach installiert werden. Weitere Informationen sind in der Hilfe zur gewählten Anti-Viren-Software zu finden.

Zur Übung: Führen Sie den kostenfreien Computercheck von Deutschland sicher im Netz e.V. durch. Er erkennt Sicherheitsprobleme auf dem Gerät und hilft bei der Behebung gefundener Fehler.
www.sicher-im-netz.de/dsin-computercheck

2

Browser & Suchmaschinen

2

Browser & Suchmaschinen: Die richtigen Informationen finden

Wie funktionieren Internetbrowser? Was ist bei der Recherche mit Suchmaschinen zu beachten? Und warum speichern Websites Daten? Um uneingeschränkt und unbeobachtet im Internet zu surfen, sollten Datenspuren reduziert werden. digital verein(t) zeigt in diesem Kapitel, wie es geht.

Tipp 6 **Webbrowser und andere Programme nur von vertrauenswürdigen Quellen herunterladen.**

Die Logos der bekanntesten Browser

Die bekanntesten Webbrowser sind Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Opera und Brave. Diese Programme sind kostenfrei und können auf den Hersteller:innenseiten sowie auf den Seiten seriöser Fachportale heruntergeladen werden.

Ein **Browser** (von „to browse", auf Deutsch: stöbern oder umsehen) ist ein Computerprogramm, das Websites grafisch darstellt. Im Browser sind also keine Algorithmen und Codes, sondern Texte, Bilder und Links zu sehen. Wenn nacheinander verschiedene Links als Verbindung zwischen verschiedenen Websites aufgerufen werden, nennt man das „Surfen".

Programme und Apps sollten idealerweise direkt von den Seiten der Hersteller:innen heruntergeladen werden. Eine Alternative sind seriöse Fachportale wie zum Beispiel heise Download. Das Portal wird von der Heise Gruppe in Hannover verantwortet und bietet rund 30.000 Software-Titel zum Herunterladen an. Nach Themen vorstrukturierte Kategorien und eine Suchfunktion erleichtern das Auffinden geeigneter Software. Kommentare anderer Nutzer:innen und Hintergrundberichte auf dem eingebetteten Blog helfen zu beurteilen, ob die Software den gewünschten Zwecken entspricht.
www.heise.de/download

Browser-Einstellungen

Jeder Browser verfügt über andere Einstellungsmöglichkeiten. Diese befinden sich meistens im Menü (unter dem auch als „Hamburger-Menü-Icon" bezeichneten Symbol aus drei Strichen) unter dem Titel „Einstellungen" oder „Über diesen Browser" beziehungsweise unter dem Zahnrad-Symbol. Wenn ein Browser heruntergeladen wurde, sollten zuerst die **Sicherheitseinstellungen** im Browser gesucht und überprüft werden.

Vielleicht ist es schon vorgekommen, dass Ihnen beim Ausfüllen eines Online-Formulars automatisch Eingabetexte vorgeschlagen wurden, zum Beispiel die E-Mail-Adresse oder der Nachname. Dafür sorgen Cookies. Cookies helfen dabei, wiederkehrende Handlungen auf Websites zu erleichtern, indem sie beispielsweise Passwörter, Spracheinstellungen, Onlineshopping-Präferenzen oder Adressdaten bei Bestellungen speichern. So müssen Nutzer:innen nicht immer wieder alle Daten neu eingeben.

Cookies (auf Deutsch: Kekse, denn wie Kekskrümel legen Cookies eine verfolgbare Datenspur im Internet) sind Dateien im Browser, die speichern, welche Websites von den Nutzer:innen mit welchen Einstellungen besucht wurden.

Diese Datenspuren werden allerdings auch für Werbezwecke genutzt. Sie helfen Unternehmen, das Surfverhalten der Nutzer:innen zu analysieren, um ihnen passgenaue **Werbung** zu präsentieren. Werden die Daten aus den Cookies mit einer E-Mail-Adresse oder einem Namen kombiniert (was ohne Einwilligung der Nutzer:innen grundsätzlich nicht erlaubt ist), können Rückschlüsse auf die Lebenssituation oder Pläne von Nutzer:innen gezogen werden. Wenn mehrere Personen über dasselbe Benutzerkonto Zugang zu einem Vereinscomputer haben, können Cookies auch die persönlichen Interessen der anderen Nutzer:innen verraten.

Tipp 7

Regelmäßig den Browserverlauf und Cache-Speicher löschen.

Im **Browserverlauf** wird gespeichert, welche Websites zuletzt aufgerufen wurden. Wer nicht möchte, dass andere Nutzer:innen des gleichen Geräts das Surfverhalten nachvollziehen können, sollte den Browserverlauf regelmäßig löschen oder im privaten Modus surfen, damit kein Browserverlauf angelegt wird.

Der sogenannte **Cache** ist vergleichbar mit einem Zwischenspeicher: Er speichert temporär Informationen von aufgerufenen Websites. Dadurch verkürzen sich die Ladezeiten dieser Websites beim wiederholten Aufruf. Wer aufgerufene Seiten aus dem Speicher entfernen will, sollte neben dem Browserverlauf also auch den Cache regelmäßig löschen. Durch das Löschen wird außerdem sichergestellt, dass beim Aufruf immer die jeweils aktuelle Seitenversion geladen wird und keine veraltete Seite aus dem Zwischenspeicher hervorgeholt wird.

Löschen von Browserdaten

Das Löschen von Cookies, Verlauf und Cache ist nicht schwer, funktioniert allerdings in jedem Browser ein wenig anders. Am Beispiel von Google Chrome und Firefox, den 2024 in Deutschland am meisten genutzten Webbrowsern, erklärt digital verein(t) in einzelnen Schritten, wie das geht. Aktuelle Anleitungen zum Löschen von Daten im Browser können im Internet recherchiert werden, wenn beispielsweise nach den Stichworten „Browserdaten löschen Safari“ gesucht wird.

Löschen von Browserdaten in Google Chrome:

1. In der Symbolleiste des Browsers oben rechts auf das Chrome-Menü klicken.

2. Auf „Browserdaten löschen“ klicken.

3. Unter dem Reiter „Erweitert“ mithilfe der Checkboxen alle Daten auswählen, die gelöscht werden sollen (Browserverlauf, Downloadverlauf, Cookies, Passwörter etc.). Oben in der Auswahl kann außerdem der Zeitraum bestimmt werden, für den die Informationen entfernt werden sollen.

4. Wenn im Chrome-Menü auf „Einstellungen“ geklickt wird, sind unter „Datenschutz und Sicherheit“ Einstellungsmöglichkeiten zu finden, um das Speichern von Daten zu vermeiden. Unter „Inhaltseinstellungen“ kann beispielsweise festgelegt werden, welche Informationen nicht von Websites genutzt werden dürfen.

Löschen von Browserdaten in Firefox:.

1. In der Symbolleiste des Browsers oben rechts im Menü (Hamburger-Menü-Icon) auf „Einstellungen“ klicken.

2. „Datenschutz & Sicherheit“ auswählen.

3. Unter „Cookies und Website-Daten“ den Button „Daten entfernen“ auswählen und nach Auswahl der Checkboxen „Leeren“ klicken. Außerdem kann mit der Wahl der Checkbox „Cookies und Webseite-Daten beim Beenden von Firefox löschen“ das Speichern von zukünftigen Browserdaten vermieden werden.

4. Unter „Chronik“ auf „Chronik leeren“ klicken. Dies öffnet ein Fenster mit Checkboxen. Oben den Zeitraum und über die Checkboxen auswählen, welche Daten gelöscht werden sollen. Abschließend auf „Jetzt löschen“ klicken.

5. Außerdem in der Auswahl unter „Chronik“ festlegen, dass zukünftig keine Chronik mehr angelegt werden soll.

Überblick über die verschiedenen Suchmaschinen

Recherchieren mit Suchmaschinen

Das Internet besteht aus mehreren Milliarden Websites. Wer hier nach bestimmten Inhalten sucht, startet deshalb in der Regel mit einer Suchmaschine. Das ist eine Internetseite mit einem Eingabefeld, in das ein bestimmter **Suchbegriff** oder mehrere Begriffe eingegeben werden können. Innerhalb weniger Sekunden erscheint eine Ergebnisliste der herausgefilterten Websites, Dokumente, Bilder und Videos. Auch hier sind einige Sicherheitsaspekte zum Schutz von Daten zu beachten.

Tipp 8 / Sicherheitseinstellungen in den genutzten Suchmaschinen überprüfen.

Auch Suchmaschinen haben Sicherheitseinstellungen, die im Menü unter „Einstellungen“ zu finden sind. Hier lassen sich je nach Anbieter verschiedene Einstellungen vornehmen. Dabei sollte vorab überlegt werden, was wichtig ist: Sollen Suchbegriffe nicht jedes Mal wieder neu eingegeben werden? Oder soll vielmehr der Suchverlauf nicht sicht- beziehungsweise nachvollziehbar sein?

Die in Deutschland am meisten genutzten **Suchmaschinen** sind Google und Bing. Daneben gibt es viele weitere Anbieter wie beispielsweise DuckDuckGo, die als besonders datenschutzfreundlich gilt; Ecosia, die sich durch besonderen Umweltschutz im Betrieb auszeichnet; oder Startpage, die Google als Algorithmus nutzt, aber die Anfragen anonymisiert. Außerdem gibt es spezielle Suchmaschinen für Kinder wie beispielsweise fragFinn.

Die Nutzung von Suchmaschinen funktioniert immer nach demselben Prinzip:

1. Auf der Startseite einer Suchmaschine befindet sich ein Eingabefeld, in das ein oder mehrere Suchbegriffe eingegeben werden. Es ist unerheblich, ob die Suchbegriffe klein oder groß geschrieben werden. Bei Tippfehlern macht die Suchmaschine Vorschläge.

2. Über den Klick auf eine Schaltfläche oder die Eingabetaste wird die Suche gestartet.

3. Die Suchmaschine liefert eine Liste von Verweisen auf möglicherweise relevante Ergebnisse. Diese sind jeweils mit Titel und einer kurzen Beschreibung oder auch Vorschaubildern dargestellt.

Vorab gilt es immer die Seriosität der Quellen zu überprüfen. Nicht alles, was im Internet zu finden ist, entspricht der Wahrheit beziehungsweise ist professionell recherchiert oder erstellt worden. Für die Glaubwürdigkeit einer Website spricht, wenn es eindeutige Verweise auf ihre Autor:innen und Betreiber:innen gibt. Diese sollten im **Impressum** zu finden sein. Außerdem ist die Aktualität ein wichtiges Kriterium, das zum Beispiel anhand des Datums von Einträgen oder Meldungen überprüft werden kann oder durch die Gültigkeit der eingebundenen Links. Wenn viele dieser Verweise auf andere Websites ungültig sind, wird die Seite nicht regelmäßig überarbeitet.

Tipp 9 / **Beim Anklicken des Suchergebnisses zwischen Werbung und Information unterscheiden.**

Die Nutzung von Suchmaschinen ist kostenfrei. Das ist möglich, weil sich die Betreiber:innen über eingeblendete Werbung finanzieren. In den Ergebnissen werden deshalb nicht nur die gewünschten Suchergebnisse angezeigt, sondern auch **Werbeanzeigen**. Diese sind – wie in Zeitschriften – als solche gekennzeichnet und heben sich in der Ansicht zum Beispiel farblich von den eigentlichen Suchergebnissen ab. Oft erscheinen sie auch am Rand des Bildschirmfensters. Bei der Recherche sollte also darauf geachtet werden, dass möglicherweise besser das Suchergebnis und nicht eine Werbung angeklickt wird.

Werbende zahlen einen bestimmten Geldbetrag an das Unternehmen, das die Suchmaschine betreibt, damit sie ganz oben in der Ergebnisliste zu bestimmten Suchbegriffen erscheinen. Deshalb passen die Anzeigen auch immer zu den eingegebenen Suchbegriffen. Einige Suchmaschinen passen die Ergebnisanzeige auch individuell an. So werden beispielsweise Nutzer:innen in Hamburg bei der Suche nach italienischen Restaurants andere Ergebnisse angezeigt als Nutzer:innen in München. Die Präferenzen und Aufenthaltsorte können in den Sicherheits- und Datenschutzeinstellungen des Geräts und der Suchmaschine vorgenommen werden.

Zur Übung: Bei der nächsten Internetrecherche den gleichen Suchbegriff mit drei verschiedenen Suchmaschinen recherchieren. Wie schneiden die Ergebnisse im Vergleich ab? Welche Einträge sind Werbung?

So funktioniert Werbung im Internet

Nicht nur Browser und Suchmaschinen verdienen ihr Geld mit Werbung. Auch viele soziale Netzwerke, Spiele und Zeitungen sind nur deshalb vermeintlich kostenlos, weil Unternehmen Werbeplätze auf den Websites buchen. Eine Werbeanzeige ist attraktiv, wenn eine möglichst große Anzahl von Menschen die Anzeige sieht oder wenn sie hauptsächlich Personen erreicht, die für das Unternehmen als potenzielle Kundschaft besonders interessant sind.

Die Websitebetreiber:innen müssen dafür wissen, wie viele Menschen ihren Service nutzen, beziehungsweise wer genau ihre Nutzer:innen sind. Dazu ermitteln sie deren Interessen und Kommunikationsgewohnheiten unter anderem anhand der Websites, die aufgerufen werden. Mit diesen Informationen können sie die Anzeigen der Werbenden gezielt ausspielen, beispielsweise Tierfutterwerbung an Personen, die schon einmal nach Tiernahrung gesucht haben. Das lässt sich vermeiden, indem der Cache regelmäßig gelöscht und die Cookie-Einstellungen in Browser und Suchmaschine angepasst werden. Wenn keine oder nur bestimmte Cookies akzeptiert werden, geht zwar die Bequemlichkeit teilweise verloren, es lassen sich dafür aber keine Cookie-basierten Profile anlegen.

Tipp 10 / **Unbedingt einen Tracking-Blocker installieren.**

Das scheint zunächst fair zu sein: Die Webservices sind kostenlos und die einzige Gegenleistung ist die Anzeige von Werbung, die sogar den eigenen Interessen entspricht. Aber oft ist nicht transparent, welche Daten

die Anbieter sammeln, wie lang sie diese speichern und wer auf die Daten zugreifen kann. Durch dieses sogenannte **Tracking**, dem Verfolgen der Internet-Nutzer:innen durch kleine Spionageprogramme, entstehen riesige Mengen an Informationen über die Nutzer:innen. Mithilfe von Browsererweiterungen, den sogenannten **Add-ons** oder **Plug-ins** lassen sich Datenspuren beim Surfen verwischen. Tracking-Blocker werden direkt in den Browser integriert und verhindern, dass personalisierte Werbung angezeigt wird.

Je nach Browser können verschiedene Add-ons eingerichtet werden, die von seriösen Plattformen heruntergeladen werden sollten.

Der **Brave-Browser** zielt darauf ab, das Tracking von Benutzerdaten zu minimieren und das Online-Privatsphäreniveau zu maximieren. Zudem verfügt er über eine integrierte Tor-Unterstützung, die dabei hilft, anonym im Internet zu surfen.
www.brave.com

Der von der Stiftung Warentest getestete Tracking-Blocker **uBlockOrigin** schützt effektiv vor Tracking, Schadsoftware und Werbung. Dabei kommt es nicht zu Funktionsverlusten oder zu einer Verlangsamung des Ladevorgangs von Websites. Die Handhabung wurde sowohl für Normalnutzer:innen als auch für erfahrene Nutzer:innen als sehr gut bewertet. Der Tracking-Blocker ist für die meisten gängigen Browser verfügbar.

Im Browser kann auch der Privat- oder Inkognito-Modus eingestellt werden. Das bedeutet, dass keine Cookie-Daten erhoben werden und der Browser die besuchten Websites nicht im Verlauf abspeichert. Bei Google Chrome kann im Inkognito-Modus gesurft werden, wenn auf das Chrome-Menü geklickt und „Neues Inkognito-Fenster“ ausgewählt wird. Bei Mozilla Firefox gibt es zum privaten Browsen ein sogenanntes „Privates Fenster“: Dazu rechts oben auf das Menü-Symbol klicken und „Privates Fenster“ auswählen.

Zur Übung: Herausfinden, wie die gewählte Suchmaschine Daten verwendet. Wie verständlich sind die Allgemeinen Geschäftsbedingungen (AGB)? Wenn die AGB aufgrund juristischer Fachbegriffe kaum verständlich sind, sollte im Internet nach Informationen gesucht werden. Dazu den Namen des Dienstes und weitere Stichwörter wie „Datenschutz“ oder „Sicherheit“ in eine Suchmaschine eingeben und auf einen nicht-werblichen Artikel eines Fachmagazins oder einer Tageszeitung klicken. Die meisten Internetangebote werden regelmäßig getestet und Aktualisierungen von AGB gut verständlich aufbereitet.

Tipp 11 / Regelmäßig die Sicherheitseinstellungen von sozialen Netzwerken kontrollieren.

Auch in sozialen Netzwerken sollte dringend auf die Privatsphäre geachtet werden. So können die eigenen sowie die Daten anderer geschützt werden. Persönliche Daten von Vereinsmitgliedern, wie beispielsweise Telefonnummern oder Adressen, sollten nie öffenltich gepostet werden. Dazu gehört außerdem, niemals Informationen über den eigenen oder den Aufenthaltsort anderer öffentlich im Netz zu nennen.

Ausführlichere Informationen zur **sicheren Kommunikation** per E-Mail, Messenger und in sozialen Netzwerken gibt es in den digital verein(t)-Handbüchern „Online-Kommunikation: Mailen, Messenger nutzen und Videoanrufe starten“ sowie „Soziale Netzwerke kennenlernen: Erste Schritte und Sicherheit“.

3

Apps & WLAN

3

Apps & WLAN: Von überall sicher ins Internet

Wenn der Verein bei Vereinsfesten oder Sitzungen ein WLAN für Gäste zur Verfügung stellen möchte, dann sollten folgende Fragen vorab besprochen werden: Was ist bei der Installation von Apps zu beachten? Wie kann kostenfreies Internet via WLAN sicher genutzt werden? Und wo kann man sich über aktuelle Sicherheitslücken informieren? Um alle Vorteile des mobilen Internets zu genießen, sind einige Grundregeln zu beachten. digital verein(t) zeigt in diesem Kapitel, wie es geht.

Tipp 12 / **Sensible Daten nur über verschlüsselte WLAN-Verbindungen verschicken.**

Das WLAN-Symbol

Wer unterwegs in einem öffentlichen WLAN surft, dem sollte bewusst sein, dass die eigenen Daten hier unsicherer sind als im privaten Netz zuhause oder im Vereinsheim. Denn Nutzer:innen können weder wissen noch überprüfen, wie gut beispielsweise im Restaurant oder im Hotel das WLAN gesichert und verschlüsselt ist. Wenn in öffentlichen Netzen gesurft wird, sollten daher zwei wichtige Verhaltensregeln beachtet werden:

- Nur E-Mail- und Messenger-Dienste mit Ende-zu-Ende-Verschlüsselung verwenden. Das bedeutet, dass die übertragenen Daten nur von den Kommunikationspartner:innen entschlüsselt werden können.
- Auf sensible Transaktionen wie Onlinebanking und -shopping mit Eingabe von Zahlungsdaten verzichten.

WLAN (= Wireless Local Area Network, auf Deutsch: drahtloses lokales Netzwerk) ist ein kabelloses Funknetzwerk zur lokalen Übertragung von Daten.

Ausführlichere Informationen zu verschlüsselter Kommunikation sind im digital verein(t)-Handbuch „Online-Kommunikation: Mailen, Messenger nutzen und Videoanrufe starten“ zu finden. Für mehr Details zum Einkaufen im Internet kann im digital verein(t)-Handbuch „Finanzen im Netz: Gelder verwalten, online einkaufen und bezahlen“ nachgeschaut werden.

VPN-Verbindungen ermöglichen über private Netzwerke den sicheren Zugriff auf das Internet.

Wenn regelmäßig in öffentlichen und gewerblichen Netzen gesurft wird, sollte für die Verbindung ein **VPN-Client** genutzt werden. Dafür muss eine VPN-Software auf dem Gerät installiert werden. Hier gibt es sowohl kostenpflichtige als auch kostenfreie Dienste.

Ein Virtual Private Network (kurz: **VPN**, auf Deutsch: virtuelles privates Netzwerk) ist ein Netzwerk, in dem Daten verschlüsselt über das Internet versendet und empfangen werden. Neben der anonymen Online-Kommunikation ermöglicht VPN auch den Zugriff auf das interne Netzwerk eines Unternehmens, Vereins oder anderer Organisationen, so dass Mitarbeitende ortsunabhängig auf Daten zugreifen können.

Die kostenlose Version von Avira Phantom VPN verschlüsselt den Datenverkehr und ermöglicht so das private Surfen. Der VPN-Dienst kann auf mehreren Geräten gleichzeitig genutzt werden und wird von allen gängigen Betriebssystemen unterstützt. Mit der kostenlosen Version steht monatlich ein Datenvolumen von 500 MB für die Nutzung zur Verfügung. Personen, die viel Datenvolumen benötigen, sollten daher auf andere Dienste ausweichen.
www.avira.com/de/free-vpn

Im Opera-Browser ist ein kostenloser VPN-Dienst integriert. Dieser kann ganz einfach über die Sicherheitseinstellungen des Browsers aktiviert werden. Sobald dies einmal erfolgt ist, wird in der Adresszeile des Browsers ein kleines Symbol für das VPN angezeigt. Zum Aktivieren oder Deaktivieren des VPN-Dienstes reicht dann ein Klick auf das entsprechende Symbol.
www.opera.com/de/computer/features/free-vpn

Tipp 13 / Das WLAN durch ein Passwort und Gastzugänge absichern.

Ein WLAN, das für eine unbestimmte Anzahl an Personen eingerichtet wird, gilt als öffentlich. Wenn Vereine von einem Netzzugang profitieren und direkt oder indirekt durch das WLAN Geld einnehmen, gilt das WLAN als gewerblich und muss bei der Bundesnetzagentur angemeldet werden. Ob das Teilen des Netzes überhaupt erlaubt ist, lässt sich in den Allgemeinen Geschäftsbedingungen (AGB) des Telekommunikationsanbieters nachlesen. Damit das WLAN sicher ist, sollte auf drei Dinge geachtet werden:

- Das WLAN sollte unbedingt mit einem Passwort gesichert werden. Bei den aktuellen Routern ist eine Verschlüsselung über WPA3 bereits eingerichtet und aktiviert. Wichtig ist, dass das Passwort (auch **WLAN-Schlüssel** oder Pre-Shared Key genannt) in den Grundeinstellungen des Routers beziehungsweise in den Windows-Sicherheitseinstellungen geändert wird.

WPA3 (Wi-Fi Protected Access) ist die neueste Verschlüsselungsmethode für WLAN. Drahtlose Netzwerke werden dadurch vor dem unbefugten Zugriff geschützt, so dass ausgetauschte Daten nicht durch Dritte mitgelesen werden können.

- Mit dem Einrichten eines **Gäste-WLAN** wird ein Internetzugang zum Beispiel bei Veranstaltungen im Verein mit den Gästen geteilt. Zeitgleich werden eigene Geräte und Daten geschützt. Informationen zur Einrichtung eines solchen Gastzugangs mit eigenem Passwort sind in der Bedienungsanleitung des Routers oder online zu finden.

- Nutzer:innen sollten zu einem verantwortungsbewussten Umgang mit rechtlich geschützten Inhalten aufgefordert werden. Vereine können dafür eine **Nutzungsvereinbarung mit den Mitgliedern** abschließen oder eine allgemeine WLAN-Ordnung aushängen.

Alle Informationen zur Anmeldung eines öffentlichen WLAN können bei der Bundesnetzagentur aufgerufen werden.
www.bundesnetzagentur.de

Auf den Seiten der Verbraucherzentrale gibt es Informationen über die rechtlichen Bedingungen von öffentlichen Netzwerken.
www.verbraucherzentrale.de

Installation von Apps

Apps werden über spezielle Vertriebsplattformen wie dem App Store (bei Apple-Geräten) und dem Play Store (bei Android-Geräten) oder über Websites heruntergeladen und auf mobilen Geräten installiert. Um diese kleinen Programme unterwegs sicher zu nutzen, sollte für Smartphones und Tablets sowie für jede einzelne der Apps Sicherheitseinstellungen vorgenommen werden.

Apps beziehungsweise Application Software (auf Deutsch: Anwendungsprogramme) sind kleine Computerprogramme mit einem bestimmten Zweck. Es gibt Apps für den Fahrplan und Ticketkauf im Öffentlichen Nahverkehr, Apps für die Wettervorhersage, für soziale Netzwerke, E-Mail-Programme, Spiele und vieles mehr.

Tipp 14 **Apps nur aus offiziellen App Stores oder von seriösen Internetseiten herunterladen.**

Es ist wichtig, Apps von vertrauenswürdigen Quellen wie dem App Store oder den Websites etablierter Fachmagazine zu beziehen. Hier kann man davon ausgehen, dass die verfügbaren Apps vom Hersteller des Betriebssystems auf Sicherheit überprüft wurden. Die am weitesten verbreiteten Betriebssysteme für Smartphone sind Android und iOS. Zur Grundausstattung gehört in der Regel ein eigener App Store, über den zum Betriebssystem passende Apps heruntergeladen werden können. Nicht alle Apps sind für jedes Betriebssystem verfügbar. So kann es vorkommen, dass eine App auf dem iPhone (Betriebssystem iOS) installiert ist, aber nicht auf dem Android-Gerät im Play Store heruntergeladen werden kann.

Tipp 15 **Immer kritisch überprüfen, welche Zugriffe die Apps auf das Smartphone verlangen.**

Beim Download einer App ist es wichtig, darauf zu achten, was die jeweilige App auf dem Gerät „darf". So muss beispielsweise ein Routenplaner keinen Zugriff auf das Telefonbuch oder die SMS-Funktion des Geräts bekommen. Diese Informationen benötigt der Dienst nicht, um den richtigen Weg zu berechnen. Außerdem sollte vor jedem Download in den AGB zumindest der Teil gelesen werden, in dem steht, was mit den Daten geschieht. Unter „Einstellungen" finden sich zudem zahlreiche Optionen für die Einrichtung von „Sicherheit", „Personalisieren", „Apps" und „Standort". Dahinter verbergen sich Möglichkeiten, Einfluss auf Datenspuren zu nehmen.

Zur Übung: Auf welche Daten haben die Apps auf dem Smartphone Zugriff? Über die Einstellungen lässt sich herausfinden, welche Freigaben und Erlaubnisse eingestellt sind.

Tipp 16 **Immer PIN und Sperrcode zum Schutz des Smartphones oder Tablets verwenden.**

Die PIN (= Persönliche Identifikationsnummer) für die SIM-Karte sollte genau wie Passwörter niemals preisgegeben werden, gespeichert oder offen aufgeschrieben werden. Eine PIN stellt sicher, dass nur berechtigte Personen mit dem Gerät surfen und telefonieren können. Sie wird jedes Mal eingegeben, wenn das Gerät gestartet wird. Die PIN ist zunächst von der Netzbetreiberfirma festgelegt, kann aber nach eigenem Belieben verändert werden.

Außerdem sollte der Gerätesperrcode immer aktiviert sein. Mit diesem Code kann auf die Funktionen des Geräts zugegriffen werden. Er wird jedes Mal eingegeben, wenn das Gerät angeschaltet oder nach einer Nutzungspause wieder aktiviert wird. Sperrcodes werden jeweils von den Geräteinhaber:innen eingerichtet und können geändert werden. Inzwischen ist die Entsperrung von Geräten auch durch Fingerabdruck oder Gesichtserkennung möglich.

PIN und Sperrcode sorgen dafür, dass das Gerät bei Diebstahl nicht oder nur mit großem Aufwand benutzt werden kann. Der Code sollte leicht zu merken, aber nicht zu offensichtlich sein. Die Kombination „1-2-3-4“ ist beispielsweise sehr unsicher. Daher sollte eine willkürliche Abfolge von Zahlen verwendet werden, die nicht mit persönlichen Daten wie dem Geburtsdatum in Verbindung gebracht werden kann.

Die SiBa-App, das Sicherheitsbarometer von Deutschland sicher im Netz e.V.

SiBa-App: Das Sicherheitsbarometer

Trotz privater und öffentlicher Sicherheitsmaßnahmen warnen Medien regelmäßig vor neuen Sicherheitslücken oder Computerviren. Was für die eigene Situation wirklich relevant ist, lässt sich oft schwer einschätzen. Hier hilft die SiBa-App, das Sicherheitsbarometer von Deutschland sicher im Netz e.V.
Die App bietet folgende Funktionen:

- Informationen über Spam-Wellen, Viren, kritische Sicherheitslücken und andere Bedrohungen in verbreiteten Programmen und Diensten;
- erste Handlungsempfehlungen und Sicherheitstipps;
- Unterscheidung der Gefährdungslage in einzelnen Meldungen nach dem Ampelsystem in Grün, Gelb und Rot;
- Push-Nachrichten über neue Meldungen auf Wunsch;
- Filtern zur Eingrenzung der Benachrichtigungen auf spezielle Themenbereiche;
- Möglichkeit zur direkten Weiterleitung von Meldungen an Freunde und Bekannte.

Das Sicherheitsbarometer gibt es als App kostenfrei für Android, iOS und Windows Phone. Die SiBa-App kann aus dem App Store heruntergeladen werden. Weitere Informationen zur App sind auch auf der Seite von Deutschland sicher im Netz e.V. zu finden.
www.sicher-im-netz.de/sicherheitsbarometer

Checkliste

16 Tipps: Online – aber sicher!

- **Tipp 1**
  Mit den eigenen Daten und Daten anderer sparsam umgehen.
- **Tipp 2**
  Sichere Passwörter aus Buchstaben, Zahlen und Sonderzeichen erstellen.
- **Tipp 3**
  Für jede Anwendung ein anderes sicheres Passwort verwenden.
- **Tipp 4**
  Geräte mit einem Anti-Viren-Programm und einer Firewall vor Schadsoftware schützen.
- **Tipp 5**
  Das Betriebssystem und die Software regelmäßig aktualisieren.
- **Tipp 6**
  Webbrowser und andere Programme nur von vertrauenswürdigen Quellen herunterladen.
- **Tipp 7**
  Regelmäßig den Browserverlauf und Cache-Speicher löschen.
- **Tipp 8**
  Sicherheitseinstellungen in den genutzten Suchmaschinen überprüfen.
- **Tipp 9**
  Beim Anklicken des Suchergebnisses zwischen Werbung und Information unterscheiden.
- **Tipp 10**
  Unbedingt einen Tracking-Blocker installieren.
- **Tipp 11**
  Regelmäßig die Sicherheitseinstellungen von sozialen Netzwerken kontrollieren.
- **Tipp 12**
  Sensible Daten nur über verschlüsselte WLAN-Verbindungen verschicken.
- **Tipp 13**
  Das WLAN durch ein Passwort und Gastzugänge absichern.
- **Tipp 14**
  Apps nur aus offiziellen App Stores oder von seriösen Internetseiten herunterladen.
- **Tipp 15**
  Immer kritisch überprüfen, welche Zugriffe die Apps auf das Smartphone verlangen.
- **Tipp 16**
  Immer PIN und Sperrcode zum Schutz des Smartphones oder Tablets verwenden.

Weitere Themen und Informationen unter:
www.digital-vereint.de

Über uns und unsere Partner:innen

Gefördert durch
Bayerisches Staatsministerium für Digitales

Das **Bayerische Staatsministerium für Digitales** wurde im Zuge der Regierungsbildung am 12. November 2018 neu gegründet. Es ist Denkfabrik der Digitalisierung in Bayern und kümmert sich um Grundsatzangelegenheiten, Strategie und Koordinierung. Das Digitalministerium ist das erste dieser Art in Deutschland. Damit unterstreicht Bayern die fundamentale Bedeutung des digitalen Wandels.

Das Digitalministerium steht für die Entschlossenheit, den weltweiten digitalen Entwicklungen nicht nur zu folgen, sondern sie souverän mitzugestalten. Bayerns starke Wirtschaft, innovative Wissenschaft und Forschung und die engagierten Bürger werden dabei eng eingebunden.
www.stmd.bayern.de

DsiN Deutschland sicher im Netz

Deutschland sicher im Netz e.V. (DsiN) wurde 2006 als Verein auf dem ersten Nationalen IT-Gipfel (heute: DigitalGipfel) gegründet. Als gemeinnütziges Bündnis unterstützt DsiN Verbraucher:innen und kleinere Unternehmen im sicheren und souveränen Umgang mit der digitalen Welt. Dafür bietet der Verein konkrete Hilfestellungen sowie Mitmach- und Lernangebote für Menschen im privaten und beruflichen Umfeld an.
www.sicher-im-netz.de

Mit der **Digitalen Nachbarschaft** (DiNa) sensibilisiert Deutschland sicher im Netz e.V. Vereine, Initiativen und freiwillig engagierte Bürger:innen für die Chancen der Digitalisierung.
www.digitale-nachbarschaft.de

lagfa bayern

Die **lagfa bayern** versteht sich als Brückenbauerin zwischen Zivilgesellschaft, Staat und Wirtschaft und handelt bedarfsorientiert als Partnerin und Beraterin von Organisationen, Initiativen, öffentlicher Verwaltung, Bildungseinrichtungen und Wirtschaft. Wir schaffen also Netzwerke im Bürgerschaftlichen Engagement.

Wir wollen Menschen begeistern und ermutigen, beraten und begleiten, sich mit ihren vielfältigen Fähigkeiten, Erfahrungen und Interessen für die Gesellschaft zu engagieren.
www.lagfa-bayern.de

Kompetenzstandorte

Vor Ort ist **digital verein(t)** an 28 Kompetenzstandorten in ganz Bayern angesiedelt. Als Standorte treten Freiwilligenagenturen, Freiwilligen-Zentren und Koordinierungszentren Bürgerschaftlichen Engagements (FA/FZ/KoBE) auf, die durch die digital verein(t)-Workshops nicht nur die Digitalisierung des lokalen Ehrenamts unterstützen, sondern auch das freiwillige Engagement in seiner gesamten Vielfalt.

Freiwilligenagenturen …
- ermutigen, beraten und begleiten Freiwillige.
- informieren und qualifizieren interessierte Einsatzstellen.
- machen Öffentlichkeits- und Lobbyarbeit für das freiwillige Engagement.
- starten gemeinsam mit anderen Projekte zum freiwilligen Engagement
- organisieren Freiwilligenmessen, Freiwilligentage und vieles mehr.

www.digital-vereint.de/standorte

Mehr digitale Themen

Sie möchten sich aktuell zur digitalen Sicherheit informieren und mögliche Sicherheitsprobleme schnell beheben?

Laden Sie kostenlos die SiBa-App herunter:
www.sicher-im-netz.de/siba

Starten Sie auf Ihrem Gerät den Computercheck von Deutschland sicher im Netz e.V., um Fehler im System zu erkennen und zu beheben.
www.sicher-im-netz.de/dsin-computercheck

Sie möchten digitale Kompetenzen weitervermitteln?

Die **Cyberfibel für digitale Aufklärung** von Deutschland sicher im Netz e.V. und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist ein Handbuch für Multiplikator:innen in Vereinen, Stiftungen, Bildungseinrichtungen, Volkshochschulen oder Verbänden über grundlegende Verhaltensstandards für sicheres und selbstbestimmtes Handeln in der digitalen Welt.
www.cyberfibel.de

Der **Digital-Kompass** unterstützt Menschen mit Sinnes- und Mobilitätsbeeinträchtigungen digitale Medien und Geräte sicher und souverän zu nutzen. Angeboten werden digitale Lern-Tandems und Beratung durch qualifizierte Engagierte in Treffpunkten vor Ort.
www.digital-kompass.de

Sie interessieren sich für aktuelle digital-politische und digital-gesellschaftliche Themen?

Das **Kompetenzzentrum Öffentliche IT (ÖFIT)** vom Fraunhofer-Institut für offene Kommunikationssysteme (FOKUS) beschäftigt sich mit der Entwicklung von Informationstechnologien im öffentlichen Raum, die gesellschaftliche Lebensbereiche und Infrastrukturen zukünftig beeinflussen.
www.oeffentliche-it.de

Haben Sie noch Fragen?
Schreiben Sie eine E-Mail an:
kontakt@digital-vereint.de

Informationen zu aktuellen Veranstaltungen, Webinaren und weitere Materialien finden Sie unter:
digital-vereint.de

BSI für Bürger ist ein kostenloses Informationsangebot des Bundesamtes für Sicherheit in der Informationstechnik zum sicheren Surfen im Internet.
www.bsi-fuer-buerger.de

D3 – so geht digital ist die Plattform der Stiftung Bürgermut mit Informationen und Veranstaltungen rund um Digitalisierungsthemen für Vereine, Verbände, Initiativen und Social Start-ups.
www.so-geht-digital.de

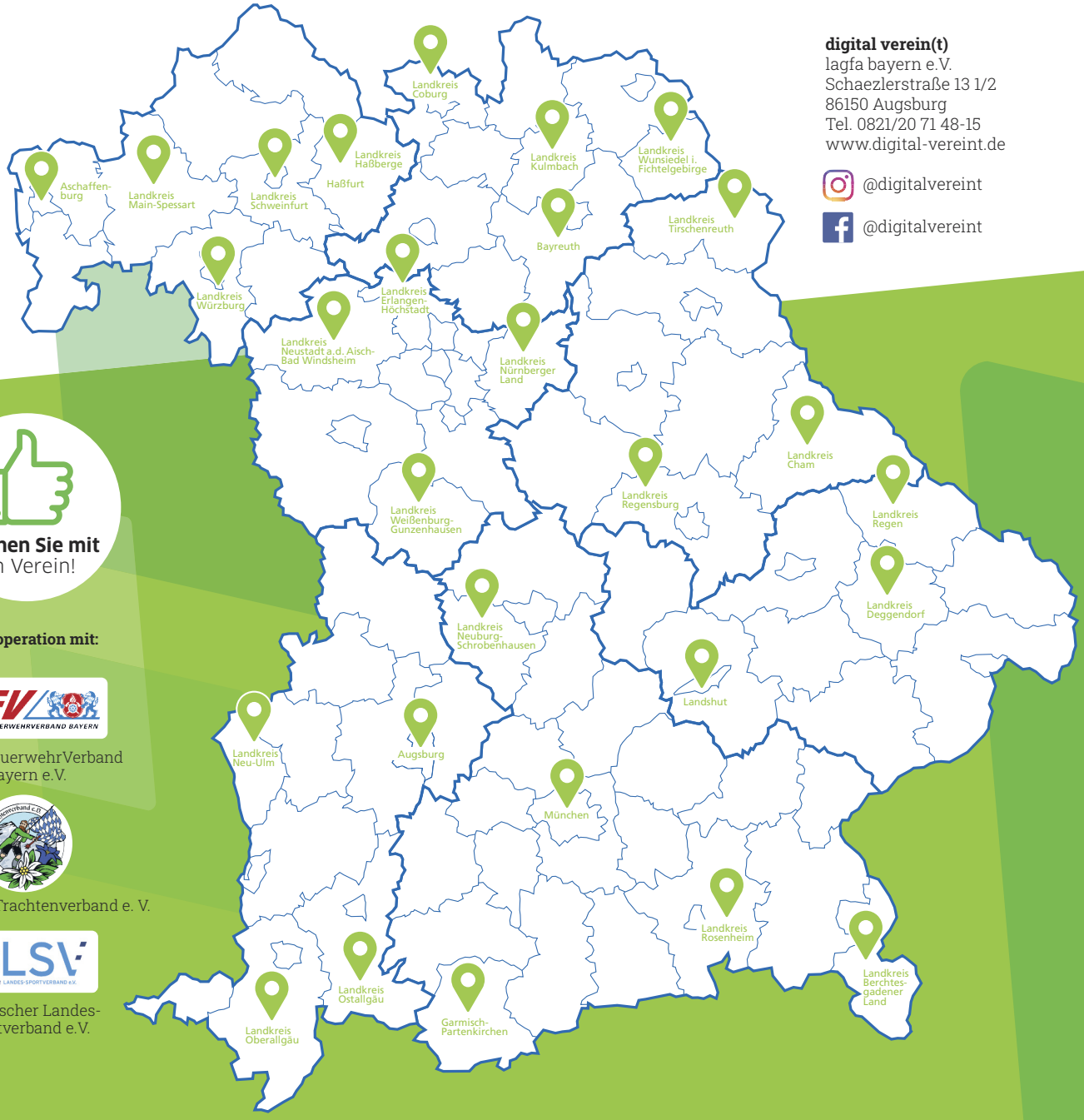
digital verein(t) vor Ort

digital verein(t)

digital verein(t)
lagfa bayern e.V.
Schaezlerstraße 13 1/2
86150 Augsburg
Tel. 0821/20 71 48-15
www.digital-vereint.de

@digitalvereint

@digitalvereint



Machen Sie mit
im Verein!

In Kooperation mit:

LandesFeuerwehrVerband Bayern e.V.

Bayerischer Trachtenverband e. V.

Bayerischer Landes-Sportverband e.V.

Freiwilligenagentur altmühlfranken
Landkreis Weißenburg-Gunzenhausen

Ehrenamtsagentur „Aschaffenburg aktiv!"

Freiwilligen-Zentrum Augsburg

Freiwilligen Zentrum Bayreuth

Freiwilligenagentur Berchtesgadener Land

Koordinierungszentrum Bürgerschaftliches Engagement „Treffpunkt Ehrenamt"
Landkreis Cham

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Coburg

mach mit – Freiwilligenzentrum Landkreis Deggendorf

Ehrenamtsbüro Landkreis Erlangen-Höchstadt

„Auf geht´s" Das Freiwilligen-Zentrum Lebenslust Garmisch-Partenkirchen e.V.

Freiwilligenagentur Mehrgenerationenhaus Haßfurt

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Kulmbach

Freiwilligen Agentur Landshut „fala"

EMiL, die Freiwilligen-Agentur Main-Spessart

Förderstelle für Bürgerschaftliches Engagement „FöBE" München

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Neuburg-Schroben-hausen

Freiwilligenagentur „Hand in Hand"
Landkreis Neu-Ulm

Freiwilligenzentrum „mach mit"
Landkreis Neustadt a.d. Aisch-Bad Windsheim

Freiwilligenzentrum WinWin
Landkreis Nürnberger Land

Freiwilligenagentur
Landkreis Oberallgäu

Servicestelle EhrenAmt
Landkreis Ostallgäu

Ehrenamtsförderung ARBERLAND
Landkreis Regen

Koordinierungszentrum Bürgerschaftliches Engagement
Freiwilligenagentur
Landkreis Regensburg

Ehrenamtskoordination
Landkreis Rosenheim

Servicestelle Ehrenamt
Landkreis Schweinfurt

Ehrenamtsagentur
Landkreis Tirschenreuth

Koordinierungszentrum Bürgerschaftliches Engagement
Landkreis Wunsiedel

Servicestelle Ehrenamt
Landkreis Würzburg