Dein Verein und seine Mitglieder

Digitale Nachbarschaft

Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen

Impressum

Redaktion: Dr. Elisabeth Maria Hofmann, Daniel Helmes (BBE), Petra Rollfing
Gestaltung und Satz: wegewerk GmbH
Erscheinungsjahr: 2019
2., durchgesehene und aktualisierte Auflage 2020: 1.000

Herausgeber: Deutschland sicher im Netz e.V.
Projekt Nachbarschaft Digital >Ehrenamt >Sicher >Transformieren
Projektleitung: Henning Baden
Geschäftsführer: Dr. Michael Littger (V.i.s.d.P.)
Albrechtstraße 10c
10117 Berlin
+49 (0) 30 767581-500
www.sicher-im-netz.de

Mit dem Projekt Nachbarschaft Digital >Ehrenamt >Sicher >Transformieren (DiNa) sensibilisiert Deutschland sicher im Netz e. V. (DsiN) Vereine, Initiativen und freiwillig engagierte Bürger*innen für die Chancen der Digitalisierung. Das Projekt verfügt über ein bundesweites Netzwerk von regionalen Anlaufstellen (DiNa-Treffs), das bedarfsgerechte Unterstützungsangebote für Bürger*innen im Ehrenamt bereitstellt. Die lokale Verankerung im vertrauten, ehrenamtlichen Umfeld fördert die nachhaltige Verbreitung von digitalen Themen im Alltag, bei denen IT-Sicherheit und Datenschutz grundlegend für ein erfolgreiches digitales Wirken im Ehrenamt sind. Mit zwei Infobussen (DiNa-Mobile) ist die DiNa auch mobil im Einsatz zu Fragen der Digitalisierung.

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).

Ein Projekt von Deutschland sicher im Netz e.V.
Gefördert durch das Bundesministerium des Innern, für Bau und Heimat
Mit Unterstützung von Deutsche Telekom AG und Deutsche Bahn AG

Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen

Handbuch der Digitalen Nachbarschaft

Die fünf Themenbereiche der Digitalen Nachbarschaft kommen direkt aus der Praxis des freiwilligen Engagements. Mit den DiNa-Handbüchern zu „Dein Verein macht sich bekannt“, „Dein Verein und seine Mitglieder“, „Dein Verein und das Geld“, „Dein Verein tauscht sich aus“ und „Dein Verein will’s wissen“ macht sich Dein Verein fit fürs Netz.

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 surft 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?

Die Digitale Nachbarschaft hat **16 DiNa-Tipps** formuliert, die Dir helfen, die digitalen Chancen für Dich und Deinen Verein sicher zu nutzen. Im ersten Kapitel geht es darum, wie Du Computer, Tablets oder Smartphones und Anwendungen sicher einrichtest. Das zweite Kapitel erläutert, wie Du im Internet surfst, ohne zu viele Informationen von Dir preiszugeben. Und schließlich zeigt Dir das dritte Kapitel, wie Du Deine persönlichen Daten schützen kannst.

In den DiNa-Häuschen findest Du kurze und praktische Hilfsmittel:

Informieren
Hier werden Fachbegriffe verständlich erklärt.

Machen
Hier werden digitale Werkzeuge vorgestellt, die Du sofort verwenden kannst.*

Üben
Hier gibt es Übungsaufgaben, um das neue Wissen anzuwenden.

Weiterlesen
Hier werden Websites und DiNa-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.

Passwörter & Firewall: Wie Du Deine Geräte absicherst

Wo Menschen zusammenkommen, um gemeinsam im Verein zu arbeiten und sich auszutauschen, entstehen schnell große Datenmengen. Warum ist Datensparsamkeit wichtig? Wie merkst Du Dir ein sicheres Passwort? Und mit welcher Software kannst Du Deine Geräte schützen? Um Geräte richtig zu bedienen und notwendige Sicherheitseinstellungen vorzunehmen, musst Du kein*e Expert*in für technische Fragen sein. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 1. Gehe sparsam mit Deinen Daten und den Daten anderer um!

Datensparsamkeit ist eine grundsätzliche Verhaltensregel im Internet. Um Deine personenbezogenen und sensiblen Daten zu schützen, solltest Du immer nur so viele Daten angeben, wie es für die jeweilige Anwendung unbedingt notwendig ist.

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 solltest Du mit **sensiblen** Daten umgehen, die als besonders schützenswert gelten. Dazu zählen beispielsweise die ethnische Herkunft, politische und religiöse Überzeugungen sowie genetische und biometrische Daten.

DiNa-Tipp

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

- Nutze beim Versand von **Rund-E-Mails** das Adressfeld „Blindkopie" (BCC). Beim Versand über das BCC-Feld 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.

- Achte bei der **Nutzung von Apps** darauf, 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.

- Vermeide es, Dich über Deine **Social-Media-Konten** für Internetdienste anzumelden. Diese können dadurch auch Deine Kontaktnetzwerke auslesen.

- Verzichte möglichst darauf, Dich bei **Internetdiensten** mit Deinem Klarnamen (das ist der bürgerliche Vor- oder Nachname) anzumelden. Es sollten außerdem nur Daten angegeben werden, die als „Pflichtfeld" gekennzeichnet sind.

- Entscheide mit Bedacht, welche **Bilder** online verfügbar sein sollen. Denn auch Fotos und Videos enthalten persönliche Informationen. Beispielsweise teilst Du mit Fotos vom Vereinsausflug auch öffentlich mit, dass das Vereinsheim gerade leer steht.

- Schalte die **Bluetooth-Funktion** aus, wenn Du sie nicht benötigst, damit andere keinen Zugang zu Deinem Gerät erhalten können.

DiNa-Tipp

DiNa-Tipp 2. Wähle sichere Passwörter, die aus Buchstaben, Zahlen und Sonderzeichen bestehen!

Ob Du mit dem PC, Tablet oder Smartphone im Internet surfst: 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 Dir, ein sicheres Passwort zu erstellen:

1. Je länger ein Passwort ist, desto sicherer ist es auch. Ein Passwort sollte aus mindestens acht Zeichen bestehen.

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

3. Benutze in Deinem Passwort keine persönlichen Daten wie Deinen Namen, Dein Geburtsdatum oder Deine Telefonnummer. Es sollte keinen Zusammenhang mit der Person haben, die es sich ausgedacht hat oder benutzt.

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

Um Dein Passwort zu schützen, solltest Du es nicht im Gerät speichern. Achte auch darauf, dass Du Dein Passwort nicht dort aufschreibst, wo es leicht auffindbar ist wie beispielsweise am Bildschirmmonitor oder im Kalender. Es ist jedoch in Ordnung, wenn Du Dein Passwort aufschreibst, in einen Briefumschlag legst und an einem sicheren Ort zuhause aufbewahrst. Außerdem gibt es hilfreiche Methoden, mit denen Du Dir Passwörter im Alltag leichter merken kannst.

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 kannst Du ein solches sicheres Passwort erstellen, das alle Sicherheitsregeln erfüllt und dennoch einfach zu merken ist. Das funktioniert so:

1. Denke Dir einen Satz mit mindestens acht Wörtern aus, in dem auch Zahlen vorkommen. Für die Wörter „ein" bzw. „eine" kann auch die Zahl „1" verwendet werden.

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

3. Schreibe auch das Satzzeichen am Ende mit auf. 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.

Überlege Dir ein sicheres Passwort mit der Merksatz-Methode. Probiere ein paar Sätze spielerisch aus. Versuche dann, ein paar Tage lang Dich immer wieder daran zu erinnern. Wenn dies gut klappt, kannst Du das Passwort sicher verwenden, ohne dass es notiert werden muss.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	G	p	6	C	w	6	O	n	7	N	g	3	1	y	5	G	e	1	T	l	5	G	y	4	J	r	1
2	9	i	0	0	&	F	1	l	Y	8	#	W	8	l	H	0	§	9	4	b	H	0	%	v	X	4	2
3	S	3	$	Z	8	&	8	5	%	F	3	§	Z	1	§	T	1	&	E	8	@	5	4	@	Z	7	3
4	#	&	J	5	#	V	l	a	N	4	#	y	6	1	E	m	o	#	4	#	i	W	j	&	0	#	4
5	r	P	u	1	t	W	z	1	j	7	u	5	j	B	v	6	n	U	s	2	n	L	d	7	u	B	5
6	4	z	9	C	y	3	F	w	4	W	g	3	E	e	6	3	j	1	S	p	9	M	e	9	I	p	6
7	1	r	L	6	#	3	6	r	V	6	§	G	2	y	T	3	&	Z	0	k	4	5	§	o	C	0	7
8	O	5	@	N	2	#	T	9	#	5	2	@	K	9	%	N	9	#	H	4	&	T	3	%	3	6	8
9	#	@	A	7	#	X	d	c	Z	2	§	i	5	S	9	d	x	%	2	@	o	A	y	§	6	&	9
10	g	Y	a	1	i	D	y	6	k	V	i	1	x	8	v	8	s	B	f	1	u	P	q	6	w	Q	10
11	E	r	7	3	z	5	B	m	7	E	c	6	D	d	0	O	h	8	5	c	8	N	c	7	I	w	11
12	3	f	I	8	&	U	4	r	3	7	#	V	2	j	T	2	@	R	6	m	Y	3	$	g	6	6	12
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	

Abbildung Passwortkarte

DiNa-Tipp

Die Passwortkarte

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

1. Wähle im Koordinatensystem einen beliebigen Startpunkt.

2. Vom Startpunkt aus nimmst Du einen „Weg" in eine beliebige Richtung. 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. Variiere Deine Passworterstellung, indem Du zum Beispiel die Zeichenfolge Deines Weges durch das Auslassen von Zeichen nach einem festen Muster verlängerst. Du kannst auch eine enthaltene Zahl ausschreiben oder jeweils den ersten und letzten Buchstaben vertauschen.

4. Jetzt musst Du Dir nur noch den Startpunkt und den Richtungsverlauf des Weges für Dein Passwort im Koordinatensystem merken. Fertig ist Dein sicheres Passwort!

DiNa-Tipp 3: Nutze für jede Anwendung ein anderes sicheres Passwort!

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 zu Deinem persönlichen E-Mail-Konto oder dem WLAN des Vereins verschafft, weiß diese Person auch das Passwort für Dein Bankkonto oder für Deine Konten in den sozialen Netzwerken. Daher solltest Du jede Anwendung mit einem eigenen Passwort schützen.

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 in Deinem Verein können sogenannte Passwort-Manager helfen. Ein Passwort-Manager speichert nicht nur Deine ganzen Passwörter, sondern kann auch sichere Passwörter für Dich erstellen. Das Programm wird durch ein Hauptpasswort, ein sogenanntes Master-Passwort, für den Zugang geschützt. Mit diesem erfolgt der Zugriff auf alle anderen Passwörter.

Der Passwort-Manager **KeePass** ist als Open Source-Programm frei verfügbar. KeePass ist ein komplexes Programm und nicht ganz intuitiv zu bedienen. Weniger geübte Nutzer*innen sollten daher eine Einarbeitungszeit einplanen. ▸ www.keepass.info/download.html

Mit der kostenlosen Version von **LastPass** kannst Du sichere Passwörter erstellen. Außerdem ist es möglich, einzelne Nutzer*innen für das LastPass-Konto freizugeben, damit diese auf die hinterlegten Passwörter zugreifen können. LastPass nutzt die sogenannte Zwei-Faktor-Authentisierung. Das bedeutet, dass neben der Eingabe des Hauptpasswortes ein zweiter Anmeldeschritt erforderlich ist, bevor Du Zugriff auf das Konto erhältst. ▸ www.lastpass.com/de

Auch **Passpack** eignet sich für die sichere Verwaltung von Passwörtern. In der kostenfreien Version lassen sich bis zu 100 Passwörter sicher speichern. Auch hier wird die Zwei-Faktor-Authentisierung eingesetzt, um das Konto doppelt vor unbefugten Zugriffen zu schützen. Das Passpack-Konto kann allerdings in der kostenlosen Variante nicht mit anderen Nutzer*innen geteilt werden. ▸ www.passpack.com/plans

DiNa-Tipp 4: Schütze Deine Geräte mit einem Anti-Viren-Programm und einer Firewall vor Schadsoftware!

DiNa-Tipp

Ausführlichere Informationen zur Zwei-Faktor-Authentisierung mit konkreten Anwendungstipps bei sozialen Netzwerken und beim Onlinebanking findest Du in den DiNa-Handbüchern „Soziale Netzwerke: Kennenlernen, nutzen, souverän kommunizieren" und „Finanzen im Netz: Online einkaufen, bezahlen und Gelder verwalten".

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.

Im Internet und in Ratgebern findest Du häufig noch die Empfehlung, Deine Passwörter regelmäßig zu ändern. 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. Schnellstmöglich ändern solltest Du Dein Passwort allerdings, wenn bekannt wird, dass Du selbst oder Dein 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).

Vor dem Online-Start solltest Du auf Deinem Gerät ein aktuelles Anti-Viren-Programm und eine Firewall einrichten. Ein Anti-Viren-Programm schützt das Betriebssystem vor schädlicher Software aus dem Internet, stärkt also sein „Immunsystem". Achte schon beim Kauf darauf, 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.

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

Überprüfe den Anti-Viren-Schutz auf Deinem Gerät und aktualisiere die Anti-Viren-Software, wenn das nötig ist.

Ist noch kein Anti-Viren-Programm und/oder keine Firewall auf Deinem Computer installiert, kannst Du im Windows Defender Sicherheitscenter oder im App Store nach geeigneten Programmen suchen. Eine weitere Möglichkeit ist, im Internet nach guten oder beliebten Programmen zu recherchieren. Etablierte Computerfachzeitschriften testen regelmäßig Anti-Viren-Programme und Firewalls. Lies auf ihren Websites nach, was unabhängige Expert*innen empfehlen.

DiNa-Tipp 5: Aktualisiere regelmäßig Dein Betriebssystem und die Software Deiner Anwendungen!

Bestimmt wurdest Du von Deinem Smartphone oder Computer schon dazu aufgefordert, Aktualisierungen, sogenannte **Updates** durchzuführen. Solche Updates schützen Deine 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 Du immer zeitnah die geforderten Updates durchführst.

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. Du findest es im Start-Menü unter „Windows-Systemsteuerung" und dann „Sicherheit und Wartung". Wenn Windows die Anti-Viren-Software erkennen kann, wird diese unter „Virenschutz" aufgelistet. Falls die Software aktualisiert werden muss, klicke auf „Jetzt aktualisieren". Bei Apple-Computern ist der Aktualisierungsstatus im **App Store** zu finden. Für manuelle Aktualisierungen klicke hier auf die angezeigten neu verfügbaren Updates und wähle dann die gewünschten Aktualisierungen einzeln oder insgesamt aus.

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 kannst Du nach dem Update für die Softwareversion im passenden Betriebssystem suchen. 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.

Der kostenfreie DsiN-Computercheck erkennt Sicherheitsprobleme auf Deinem Gerät und hilft bei der Behebung gefundener Fehler.
▸ www.sicher-im-netz.de/dsin-computercheck

2

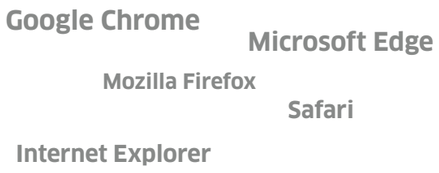
2

Browser & Suchmaschinen: Wie Du zur richtigen Info findest

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, solltest Du Deine Datenspuren reduzieren. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 6: Lade Webbrowser und andere Programme nur von vertrauenswürdigen Quellen herunter!



Die bekanntesten Browser

Die bekanntesten Webbrowser sind Google Chrome, Mozilla Firefox, Internet Explorer beziehungsweise Microsoft Edge und Safari. Diese Programme sind kostenfrei und können auf den Herstellerseiten sowie von den Seiten seriöser journalistischer Fachportale heruntergeladen werden.

i

Ein **Browser** (auf Deutsch: stöbern oder umsehen) ist ein Computerprogramm, das Websites grafisch darstellt. Du siehst im Browser also keine Algorithmen und Codes, sondern Texte, Bilder und Links. Wenn Du nacheinander beliebige Links als Verbindung zwischen verschiedenen Websites aufrufst, dann surfst Du im Internet.

Programme und Apps solltest Du idealerweise direkt von den Seiten der Hersteller herunterladen. 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 eine andere Breite an 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 Du den Browser Deiner Wahl heruntergeladen hast, solltest Du als erstes die **Sicherheitseinstellungen** im Browser suchen und überprüfen.

Wenn Du Deine E-Mail-Adresse in ein Feld eingegeben hast, ist es vielleicht schon vorgekommen, dass sie bei der nächsten Eingabe automatisch vorgeschlagen wurde. Du musstest Deine E-Mail-Adresse also nicht wieder neu eintippen, sondern konntest sie einfach auswählen. 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.

i

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 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.

DiNa-Tipp 7: Lösche regelmäßig den Browserverlauf und Cache-Speicher in den Einstellungen Deines Browsers!

Im **Browserverlauf** wird gespeichert, welche Websites Du zuletzt aufgerufen hast. Wer nicht möchte, dass andere Nutzer*innen des gleichen Geräts das Surfverhalten nachvollziehen können, sollte den Browserverlauf regelmäßig löschen. Dies ist ebenfalls über die Sicherheitseinstellungen des Browsers möglich.

Der sogenannte **Cache** ist vergleichbar mit einem Versteck: Er speichert 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 „Versteck" 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 2019 in Deutschland am meisten genutzten Webbrowsern, erklären wir Dir in einzelnen Schritten, wie das geht. Aktuelle Anleitungen zum Löschen von Daten in Deinem Browser kannst Du im Internet recherchieren, wenn Du beispielsweise nach den Stichworten „Browserdaten löschen Safari" suchst.

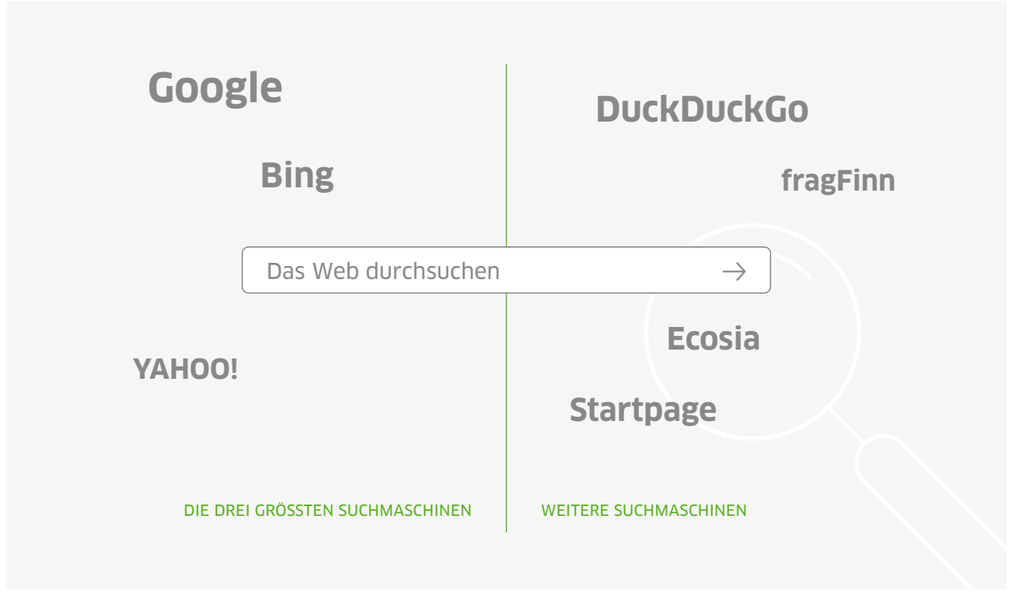
Löschen von Browserdaten in Google Chrome:

1. Klicke in der Symbolleiste des Browsers oben rechts auf das Chrome-Menü.
2. Klicke auf „Weitere Tools".
3. Klicke auf „Browserdaten löschen".
4. Wähle unter dem Reiter „Erweitert" mithilfe der Checkboxen alle Daten aus, die gelöscht werden sollen (Browserverlauf, Downloadverlauf, Cookies, Passwörter etc.). Du kannst oben in der Auswahl außerdem den Zeitraum bestimmen, für den die Informationen entfernt werden sollen.
5. Wenn Du im Chrome-Menü auf „Einstellungen" klickst, findest Du unter „Datenschutz und Sicherheit" Einstellungsmöglichkeiten, um das Speichern von Daten zu vermeiden. Unter „Inhaltseinstellungen" kannst Du beispielsweise festlegen, welche Informationen nicht von Websites genutzt werden dürfen.

DiNa-Tipp

Löschen von Browserdaten in Firefox:

1. Klicke in der Symbolleiste des Browsers oben rechts im Menü (Hamburger-Menü-Icon) auf „Einstellungen".
2. Wähle „Datenschutz & Sicherheit" aus.
3. Klicke unter „Cookies und Webseite-Daten" „Daten entfernen" und nach Auswahl der Checkboxen „Leeren". Du kannst außerdem mit der Wahl der Checkbox „Cookies und Webseite-Daten beim Beenden von Firefox löschen" das Speichern von zukünftigen Browserdaten vermeiden.



Überblick über die verschiedenen Suchmaschinen

4. Klicke unter „Chronik“ auf „Chronik leeren“. Dies öffnet ein Fenster mit Checkboxen. Wähle oben den Zeitraum und über die Checkboxen aus, welche Daten gelöscht werden sollen. Klicke abschließend auf „Jetzt löschen“.

5. Du kannst außerdem in der Auswahl unter „Chronik“ festlegen, dass zukünftig keine Chronik mehr angelegt wird.

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 Deiner Daten zu beachten.

DiNa-Tipp

DiNa-Tipp 8: Prüfe die Sicherheitseinstellungen in Deiner Suchmaschine!

Auch Suchmaschinen haben Sicherheitseinstellungen, die im Menü unter „Einstellungen“ zu finden sind. Hier lassen sich je nach Anbieter verschiedene Einstellungen vornehmen. Überlege Dir dabei, was Dir wichtig ist: Möchtest Du Suchbegriffe nicht jedes Mal wieder neu eingeben müssen? Oder willst Du vielmehr, dass Dein Suchverlauf nicht sicht- beziehungsweise nachvollziehbar ist?

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 Du die Suchbegriffe klein oder groß schreibst. Bei Tippfehlern macht die Suchmaschine Vorschläge, was wahrscheinlich gemeint sein könnte.

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.

Prüfe immer die Seriosität der Quellen. Nicht alles, was Du im Internet findest, 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 gibt. Diese sollten im **Impressum** zu finden sein. Außerdem ist die Aktualität ein wichtiges Kriterium, das Du zum Beispiel anhand des Datums von Einträgen oder Meldungen überprüfen kannst oder durch die Gültigkeit der eingebundenen Links. Wenn viele dieser Verweise auf andere Websites ungültig sind, wird die Seite nicht regelmäßig überarbeitet.

DiNa-Tipp 9: Achte auf die Unterschiede zwischen gewünschten Suchergebnissen und ungewollter Werbung!

Die Nutzung von Suchmaschinen ist kostenfrei. Das ist möglich, weil sich die Betreiber 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 solltest Du also darauf achten, ob Du ein Suchergebnis oder eine Werbung anklickst.

Unternehmen zahlen einen bestimmten Geldbetrag an den Betreiber der Suchmaschine, damit sie ganz oben in der Ergebnisliste zu bestimmten Suchbegriffen erscheinen. Deshalb passen die Anzeigen auch immer zu den eingegebenen Suchbegriffen. Einige Suchmaschinenbetreiber optimieren die Ergebnisanzeige für ihre Nutzer*innen. So werden beispielsweise Nutzer*innen aus Hamburg bei der Suche nach italienischen Restaurants andere Ergebnisse angezeigt als Nutzer*innen in München. Die Präferenzen und Aufenthaltsorte der Nutzung kannst Du in den Sicherheits- und Datenschutzeinstellungen des Geräts und der Suchmaschine vornehmen.

Überlege Dir einen Suchbegriff, teste drei verschiedene Suchmaschinen und vergleiche die Ergebnisse! Welche Einträge sind Werbung, welche nicht?

So funktioniert Werbung im Internet

Nicht nur Browser und Suchmaschinen verdienen ihr Geld mit Werbung. Auch viele soziale Netzwerke, Spiele und Zeitungen sind kostenlos, da 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.

DiNa-Tipp

Die Websitebetreiber 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 vermeidest Du, wenn Du den Cache regelmäßig löschst und die Cookie-Einstellungen in Browser und Suchmaschine anpasst. Wenn Du Cookies nicht akzeptierst, verlierst Du Bequemlichkeit, dafür lassen sich keine Profile über Dich anlegen.

DiNa-Tipp

DiNa-Tipp 10: Installiere einen Tracking-Blocker!

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 **Cliqz-Browser** ist ein separater Browser, der auf Mozilla Firefox aufbaut und die Übertragung von persönlichen Daten an Datenanalysefirmen oder Werbenetzwerke verhindert. Die Handhabung ist einfach. Er ist sowohl für Windows als auch für iOS verfügbar. ▸ www.cliqz.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 Google Chrome, Mozilla Firefox, Microsoft Edge und Safari verfügbar.

Du kannst im Browser auch den **Privat-Modus** einstellen. Das bedeutet, dass keine Cookie-Daten erhoben werden und der Browser die besuchten Websites nicht im Verlauf abspeichert. Bei Google Chrome kannst Du im Inkognito-Modus surfen, wenn Du auf das Chrome-Menü klickst und „Neues Inkognito-Fenster“ wählst. Bei Mozilla Firefox gibt es zum privaten Browsen ein sogenanntes „Privates Fenster“: Klicke dazu rechts oben auf das Menü-Symbol und wähle „Privates Fenster“.

Finde heraus, wie Deine gewählte Suchmaschine Deine Daten verwendet. Wie verständlich sind die Allgemeinen Geschäftsbedingungen (AGB) für Dich? Wenn Du die AGB aufgrund juristischer Fachbegriffe kaum verstehst, suche im Internet nach Informationen. Gib dazu den Namen des Dienstes und weitere Stichwörter wie „Datenschutz“ oder „Sicherheit“ in eine Suchmaschine ein und klicke auf einen nicht-werblichen Artikel eines Fachmagazins oder einer Tageszeitung. Die meisten Internetangebote werden regelmäßig getestet und Aktualisierungen von AGB gut verständlich aufbereitet.

DiNa-Tipp

DiNa-Tipp 11: Kontrolliere regelmäßig die Sicherheitseinstellungen von sozialen Netzwerken!

Auch soziale Netzwerke erfordern die Einstellungen der Privatsphäre. Dabei werden nicht nur die eigenen, sondern auch die Daten anderer geschützt. Du solltest daher niemals eigene oder persönliche Daten von Bekannten oder Vereinsmitgliedern wie beispielsweise Telefonnummern oder Adressen öffentlich posten. 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 DiNa-Handbüchern „Online-Kommunikation: Mailen, Messenger nutzen und Videokonferenzen veranstalten“ sowie „Soziale Netzwerke: Kennenlernen, nutzen und souverän kommunizieren“.

3

Apps & WLAN: Wie Du überall sicher ins Internet kommst

Wenn Dein Verein bei Vereinsfesten oder Sitzungen ein WLAN für Gäste zur Verfügung stellt, dann werden Dich diese Fragen besonders beschäftigen: Was ist bei der Installation von Apps zu beachten? Ist kostenfreies Internet via WLAN sicher? Und wo kannst Du Dich über aktuelle Sicherheitslücken informieren? Um alle Vorteile des mobilen Internets zu genießen, sind einige Grundregeln zu beachten. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 12: Verschicke sensible Daten nur über verschlüsselte WLAN-Verbindungen!

Das WLAN-Symbol für Funknetze und mobiles Internet

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 das Restaurant oder das Hotel das WLAN gesichert und verschlüsselt hat. Wenn Du in öffentlichen Netzen surfst, solltest Du daher zwei wichtige Verhaltensregeln beachten:

- Nutze nur E-Mail- und Messenger-Dienste mit Ende-zu-Ende-Verschlüsselung.
- Verzichte auf sensible Transaktionen wie Onlinebanking und -shopping mit Eingabe von Zahlungsdaten.

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

Ausführlichere Informationen zu verschlüsselter Kommunikation findest Du im DiNa-Handbuch „Online-Kommunikation: Mailen, Messenger nutzen und Videokonferenzen veranstalten". Für mehr Details zum Einkaufen im Internet kannst Du im DiNa-Handbuch „Finanzen im Netz: Online einkaufen, bezahlen und Gelder verwalten" nachschauen.

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

Wenn Du regelmäßig in öffentlichen und gewerblichen Netzen unterwegs bist, solltest Du für die Verbindung einen **VPN-Client** nutzen. 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 Free-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. Vielnutzer*innen sollten daher auf andere Dienste ausweichen.
▸ www.avira.com/de/avira-phantom-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 Dir 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

DiNa-Tipp 13: Sichere Dein WLAN durch ein Passwort und Gastzugänge ab!

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, ist das WLAN sogar 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, solltest Du auf drei Dinge achten:

- Schütze das WLAN mit einem Passwort. Bei den aktuellen Routern ist eine Verschlüsselung über WPA2 bereits eingerichtet und aktiviert. Wichtig ist, dass Du das Passwort (auch **WLAN-Schlüssel** oder Pre-Shared Key genannt) in den Grundeinstellungen des Routers beziehungsweise in den Windows-Sicherheitseinstellungen änderst.

WPA2 (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.

- Richte einen WLAN-Gastzugang ein. Mit einem **Gäste-WLAN** teilst Du Deinen Internetzugang zum Beispiel bei Veranstaltungen in Deinem Verein, schützt aber zugleich Deine eigenen Geräte und Daten. Informationen zur Einrichtung eines solchen Gastzugangs mit eigenem Passwort findest Du in der Bedienungsanleitung des Routers oder online.
- Fordere andere Nutzer*innen zum verantwortungsbewussten Umgang mit rechtlich geschützten Inhalten auf. Vereine können dafür eine **Nutzungsvereinbarung mit den Mitgliedern** abschließen oder eine allgemeine WLAN-Ordnung aushängen.

DiNa-Tipp

Alle Informationen zur Anmeldung eines öffentlichen WLAN findest Du bei der Bundesnetzagentur. ▸ www.bundesnetzagentur.de

Auf den Seiten der Verbraucherzentrale kannst Du Dich außerdem über die rechtlichen Bedingungen von öffentlichen Netzwerken informieren. ▸ www.verbraucherzentrale.de

Der Landessportbund Berlin bietet Vereinen eine musterhafte Nutzungsvereinbarung für die Nutzung von WLAN. Gib dazu in das Suchfeld auf der Website die Begriffe „Nutzungsvereinbarung WLAN" ein. ▸ www.lsb-berlin.net

Einen weiteren beispielhaften Vertrag, der auch in englischer und arabischer Sprache sowie auf Dari und Pashto zur Verfügung steht, findest Du auf der Website der Rechtanwaltskanzlei Wilde Beuger Solmecke. Gib dazu in das Suchfeld den Begriff „Internet-Nutzungsvertrag“ ein.
▸ www.wbs-law.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, solltest Du für Dein Smartphone und Dein Tablet sowie für jede einzelne der App-Anwendungen Sicherheitseinstellungen vornehmen.

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.

DiNa-Tipp

DiNa-Tipp 14: Lade Apps nur aus offiziellen App Stores oder von seriösen Internetseiten herunter!

Es ist wichtig, Apps von vertrauenswürdigen Quellen wie dem App Store oder den Websites etablierter Fachmagazine zu beziehen. Hier kannst Du davon ausgehen, dass die verfügbaren Apps vom Hersteller des Betriebssystems auf Sicherheit überprüft wurden. Die am weitesten verbreiteten Betriebssysteme sind Android, iOS und Windows. 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.

DiNa-Tipp

DiNa-Tipp 15: Überprüfe kritisch, welche Zugriffe Apps auf Dein Smartphone verlangen!

Beim Download einer App solltest Du darauf achten, was diese auf dem Gerät darf. So sollte 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. Lies außerdem vor jedem Download in den AGB zumindest den Teil, in dem steht, was mit Deinen 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.

Auf welche Daten haben Apps auf Deinem Smartphone Zugriff? Den Zugriff der Apps findest Du über die „Einstellungen“ heraus.

DiNa-Tipp

DiNa-Tipp 16: Nutze immer PIN und Sperrcode zum Schutz Deines Smartphones oder Tablets!

Die **PIN** (= Persönliche Identifikationsnummer) für die SIM-Karte solltest Du genau wie Passwörter niemals verraten, speichern oder offen aufschreiben. 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 zuerst von der Netzbetreiberfirma festgelegt, kann aber nach eigenem Belieben verändert werden.

Außerdem sollte der **Gerätesperrcode** immer aktiviert sein. Mit diesem Code kannst Du auf die Funktionen des Geräts zugreifen. Er wird immer eingegeben, wenn das Gerät angeschaltet oder nach einer Nutzungspause wieder aktiviert wird. Sperrcodes werden jeweils von den Geräteinhaber*innen eingerichtet und können geändert werden.

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. Wähle daher eine willkürliche Abfolge von Zahlen, 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 Dir die folgenden 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. Du kannst Dir die SiBa-App aus dem App Store Deines Gerätes herunterladen. Weitere Informationen zur App findest Du auch auf der Seite von Deutschland sicher im Netz e.V.
▸ www.sicher-im-netz.de

Platz für Deine Notizen

Platz für Deine Notizen

Platz für Deine Notizen

Dein Verein und seine Mitglieder

Checkliste

16 DiNa-Tipps: Online – aber sicher!

1. Gehe sparsam mit Deinen Daten und den Daten anderer um!
2. Wähle sichere Passwörter, die aus Buchstaben, Zahlen und Sonderzeichen bestehen!
3. Nutze für jede Anwendung ein anderes sicheres Passwort!
4. Schütze Deine Geräte mit einem Anti-Viren-Programm und einer Firewall vor Schadsoftware!
5. Aktualisiere regelmäßig Dein Betriebssystem und die Software Deiner Anwendungen!
6. Lade Webbrowser und andere Programme nur von vertrauenswürdigen Quellen herunter!
7. Lösche regelmäßig den Browserverlauf und Cache-Speicher in den Einstellungen Deines Browsers!
8. Prüfe die Sicherheitseinstellungen in Deiner Suchmaschine!
9. Achte auf die Unterschiede zwischen gewünschten Suchergebnissen und ungewollter Werbung!
10. Installiere einen Tracking-Blocker!
11. Kontrolliere regelmäßig die Sicherheitseinstellungen von sozialen Netzwerken!
12. Verschicke sensible Daten nur über verschlüsselte WLAN-Verbindungen!
13. Sichere Dein WLAN durch ein Passwort und Gastzugänge ab!
14. Lade Apps nur aus offiziellen App Stores oder von seriösen Internetseiten herunter!
15. Überprüfe kritisch, welche Zugriffe Apps auf Dein Smartphone verlangen!
16. Nutze immer PIN und Sperrcode zum Schutz Deines Smartphones oder Tablets!

Weitere Themen und Informationen unter:
► **www.digitale-nachbarschaft.de**

Mehr digitale Themen

Du möchtest Dich aktuell zur digitalen Sicherheit informieren und mögliche Sicherheitsprobleme schnell beheben?

Lade kostenlos die SiBa-App herunter:
► www.sicher-im-netz.de/siba

Starte auf Deinem Gerät den DsiN-Computercheck, um Fehler im System zu erkennen und zu beheben.
► www.sicher-im-netz.de/dsin-computercheck

Du möchtest digitale Kompetenzen weitervermitteln?

#DABEI-Geschichten ist ein Angebot der Deutschen Telekom, sich leicht verständlich, innovativ und voller praktischer Tipps mit Themen der digitalen Welt zu beschäftigen, um sie zu verstehen: von Digitaler Demokratie über Digitale Freundschaft bis hin zu Datenschutz und Datensicherheit. Wer mit Lerngruppen arbeitet, findet hier Anregungen und Tipps. Die Unterlagen stehen auch in einfacher Sprache zur Verfügung.
► dabei-geschichten.telekom.com

Die DsiN-BSI-**Cyberfibel für digitale Aufklärung** 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 engagierte Menschen, älteren Generationen die Chancen des Internets und ihrer sicheren Nutzung näher zu bringen. Im Mittelpunkt steht der Erfahrungsaustausch zur verständlichen Vermittlung für Senior*innen deutschlandweit.
► www.digital-kompass.de

Du interessierst Dich für aktuelle digitalpolitische 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

Du hast noch Fragen?

Schreibe eine E-Mail an:
dina@digitale-nachbarschaft.de

Informationen zu aktuellen Veranstaltungen, Webinaren und weitere Materialien findest Du auf unserer Website:

► **www.digitale-nachbarschaft.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

Über uns und unsere Partner

Deutschland sicher im Netz e. V.

Deutschland sicher im Netz e.V. (DsiN) wurde 2006 als Verein auf dem ersten Nationalen IT-Gipfel gegründet. Als gemeinnütziges Bündnis unterstützt DsiN Verbraucher*innen und kleinere Unternehmen im sicheren und souveränen Umgang mit der digitalen Welt. Dafür bietet der Verein in Zusammenarbeit mit seinen Mitgliedern und Partner*innen konkrete Hilfestellungen sowie Mitmach- und Lernangebote für Menschen im privaten und beruflichen Umfeld an. Schirmherr des Vereins ist der Bundesminister des Innern, für Bau und Heimat.

Das Bundesministerium des Innern, für Bau und Heimat

Die Aufgaben des Bundesministeriums des Innern, für Bau und Heimat (BMI) sind ebenso vielfältig wie verantwortungsvoll. Das Spektrum reicht von der Rolle als Hüter der Verfassung und Förderer des gesellschaftlichen Zusammenhalts über die Integration, Sportförderung des Bundes und die Informationstechnik bis hin zu den Sicherheitsaufgaben. Als „Verfassungs- und Kommunalministerium" ist das BMI für die Modernisierung von Staat und Verwaltung zuständig, aber auch für Kernfragen der staatlichen und föderalen Ordnung wie beispielsweise das Wahlrecht. Ziel der Digitalpolitik des Bundesministeriums des Innern ist es, die vielfältigen Chancen der Digitalisierung für möglichst viele Menschen zu ermöglichen und zugleich etwaige Risiken zu minimieren.

Die Deutsche Telekom AG

Die Deutsche Telekom ist eines der führenden integrierten Telekommunikationsunternehmen weltweit. Chancengleiche und aktive Teilhabe an der Informations- und Wissensgesellschaft ist der Telekom stets ein wichtiges Anliegen. Mit ihrem Angebot „Medien, aber sicher" leistet sie einen wichtigen Beitrag zur Gestaltung der Digitalisierung in der Gesellschaft, indem ein kompetenter, verantwortungsvoller und dadurch sicherer Umgang mit neuen Technologien ermöglicht werden soll. Ziel ist die Förderung von Medienkompetenz für Jung und Alt. So zeigt die Deutsche Telekom mit den #DABEI-Geschichten Möglichkeiten für Partizipation und verantwortliches Handeln im Netz auf und möchte zur kritischen Auseinandersetzung motivieren.

Das Bundesnetzwerk Bürgerschaftliches Engagement (BBE)

Das Bundesnetzwerk Bürgerschaftliches Engagement (BBE) ist ein Zusammenschluss von Akteuren (vorrangig Organisationen und Institutionen) aus Zivilgesellschaft, Wirtschaft und Arbeitsleben, aus Staat und Politik, Medien und Wissenschaft. Das übergeordnete Ziel des BBE ist es, die Bürgergesellschaft und bürgerschaftliches Engagement in allen Gesellschafts- und Politikbereichen nachhaltig zu fördern. In der Kooperation mit DsiN trägt das BBE im Projekt Digitale Nachbarschaft nachhaltig zur Förderung von Engagierten im Umgang mit den Chancen der Digitalisierung bei. Das Netzwerk versteht sich als Wissens- und Kompetenzplattform für bürgerschaftliches Engagement.

Die Deutsche Bahn

Die Deutsche Bahn ist eines der führenden Mobilitäts- und Logistikunternehmen und beschäftigt weltweit rund 330.000 Mitarbeiter – davon rund 205.000 in Deutschland. Die Bahn gestaltet und betreibt die Verkehrsnetzwerke der Zukunft. Als Mobilitätsdienstleister trägt sie eine große Verantwortung für Menschen und Güter – und das rund um die Uhr. Dabei ist Sicherheit das höchste Gut für ihre Kunden und Mitarbeiter. Gemeinsam mit Deutschland sicher im Netz e.V. unterstützt die Bahn Vereine und Initiativen im sicheren und selbstbestimmten Umgang mit dem Internet, um die Chancen der Digitalisierung zu nutzen. Dabei steht die Stärkung der IT-Kompetenz und die Befähigung rund um das Thema Mobilität im Vordergrund.

Ein Projekt von:

Deutschland sicher im Netz

Mit Unterstützung von:

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Deine DiNa ist nah dran ...

→ an Deinem Verein: Die DiNa-Treffs und DiNa-Mobile sind analoge Begegnungsorte für digitale Themen.

→ an Deinen Themen: Die DiNa-Angebote und Materialien entwickeln wir aus der Praxis des freiwilligen Engagements.

→ an Deiner Art zu lernen: Die DiNa-Workshops und Webinare zeigen die Chancen des Internets und wie Du sie sicher nutzt.

www.digitale-nachbarschaft.de

@digitalenachbarschaft