Zusammenarbeit
im Verein

digital verein(t)

Online-Kommunikation:
Mailen, Messenger nutzen und Videoanrufe starten

Impressum

Herausgeber:
Deutschland sicher im Netz e.V. (DsiN)
Projekt digital verein(t)

Projektleitung:
Dr. Nils Weichert (DsiN)

Geschäftsführung:
Dr. Michael Littger (V.i.s.d.P.)
Albrechtstraße 10c
10117 Berlin
+49 (0) 30 767581-500
www.sicher-im-netz.de

Erscheinungsjahr: 2021

Redaktion:
Dr. Elisabeth Maria Hofmann,
Bernd Schöneberg

Lektorat:
Lilian Misao Grote,
Johanna Gabriel

Gestaltung und Satz:
freistil grafik&design, München

Projektpartner:
Landesarbeitsgemeinschaft der Freiwilligenagenturen/
-Zentren/ Koordinierungszentren
Bürgerschaftliches Engagement Bayern (lagfa)

Projektleitung:
Lilian M. Grote (lagfa bayern e.V.)

Digital verein(t) in Bayern ist ein Landesprojekt im Bundesnetzwerk Digitale Nachbarschaft, das in enger Kooperation mit lagfa bayern e.V. durchgeführt wird. Das Projekt wird vom Bayerischen Staatsministerium für Digitales (StMD) gefördert. Es unterstützt ehrenamtliches Engagement und Vereine in ganz Bayern bei der sicheren und kompetenten Nutzung digitaler Angebote.

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

DsiN Deutschland sicher im Netz

In Zusammenarbeit mit

lagfa bayern

Online-Kommunikation: Mailen, Messenger nutzen und Videoanrufe starten

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.

Inhalt

Über dieses Handbuch

Wenn sich die Mitglieder des Tischtennisvereins in bester Rückschlagmanier ihre E-Mails zuspielen, sollten sie die verschiedenen Funktionen und rechtlichen Regelungen der Online-Kommunikation kennen. So können E-Mails mit Hilfe der Funktion „blind carbon copy“ an eine größere Gruppe versendet werden, ohne dass alle E-Mail-Adressen für die einzelnen Empfänger:innen sichtbar sind.

Auch gemeinsame Vorstandssitzungen profitieren von digitalen Möglichkeiten. Wenn der persönliche Austausch aus verschiedenen Gründen nicht möglich ist, kann eine Videokonferenz die Alternative sein.

Das verbale Ping Pong via Videotelefonie gelingt mit wenig Vorbereitung und mit Rücksicht auf einige Sicherheitsaspekte.

Digital verein(t) hat 10 Tipps formuliert, die helfen, die digitalen Chancen sicher in der Vereinswelt zu nutzen. Im ersten Kapitel geht es um die unterschiedlichen Möglichkeiten, E-Mails zu versenden. Im zweiten Kapitel erklärt digital verein(t), wie der Schutz vor schädlichen E-Mails gelingen kann. Im dritten Kapitel stehen die unterschiedlichen Funktionen und die sichere Nutzung von Messenger-Diensten im Mittelpunkt.

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 Webmail & E-Mail-Programme

1

Webmail & E-Mail-Programme: Mit elektronischen Nachrichten zum Ziel kommen

Welche Möglichkeiten gibt es, um eine E-Mail zu versenden? Wie sieht eine sichere E-Mail-Adresse aus? Und was bedeutet verschlüsselte Kommunikation? Um von den Vorteilen der elektronischen Post auch im Vereinsalltag und bei der Öffentlichkeitsarbeit zu profitieren, sollten zu Beginn die richtigen Entscheidungen getroffen werden. Digital verein(t) zeigt in diesem Kapitel, wie es geht.

Webmail-Dienste und E-Mail-Programme

E-Mails sind elektronische Nachrichten. Sie können neben Texten auch Bilder und andere Dateien enthalten. Der Versand und Empfang erfolgt über Webmail-Dienste oder spezielle E-Mail-Programme, die auf allen Geräten genutzt werden können. Für mobile Geräte sind meistens kostenlose Apps in den App Stores zu finden. Neue Smartphones verfügen standardmäßig über vorinstallierte E-Mail-Apps.

Zur Übung: Es ist hilfreich eine Liste mit Kommunikationsanlässen und damit zusammenhängende Aufgaben anzufertigen, die digital erledigt werden können. Dazu sollten folgende Fragen beantwortet werden: Gibt es vorinstallierte Kommunikations-Apps auf dem Smartphone? Welche Apps kommen generell in Frage oder werden bereits genutzt und warum?

Zu den am weitesten verbreiteten kostenfreien Webmail-Diensten gehören GMX, WEB.DE, Gmail und t-online. Neben diesen kostenfreien Diensten gibt es besonders datensparsame Alternativen wie Posteo oder mailbox.org, die weniger Daten erheben und speichern.

Nutzer:innen werden bei der Einrichtung des Webmail-Dienstes Schritt für Schritt durch die Anmeldung geführt, von der Eingabe der gewünschten E-Mail-Adresse bis hin zum sicheren Passwort. Dabei sollte auf Datensparsamkeit geachtet und nur die persönlichen Daten angegeben werden, die für die E-Mail-Nutzung wirklich nötig sind.

Die bekanntesten koostenfreien Wwebmail-Dienste (links) und besonders datensparsame Alternativen (links)

Ausführlichere Informationen zum Umgang mit persönlichen und sensiblen Daten sind im digital verein(t)-Handbuch „Mitgliederdaten: Schützen, verwalten und verwenden“ sowie in der multimedialen Reportage „Datenschutz und Sicherheit“ auf der Plattform > dabeigeschichten.telekom.com/ zu finden.

Die Benutzeroberfläche von Webmail-Diensten ist zumeist ähnlich aufgebaut:

Ordnerstruktur auf der linken Seite: Neben den standardisierten Ordnern „Posteingang“, „Gesendet“, „Entwürfe“ und „Papierkorb“ gibt es die Möglichkeit, eigene Ordner anzulegen. Für Vereine empfiehlt es sich, unter anderem Ordner für unterschiedliche Aufgaben, Institutionen oder Personen

anzulegen wie beispielsweise „Veröffentlichungen“, „Veranstaltungen“, „Mitglieder“ oder „Kooperationspartner“. Hierhin können eingehende E-Mails verschoben werden, um sie später leichter wiederzufinden.

Posteingang auf der rechten Seite (oder in der Mitte): Die eingegangenen E-Mails erscheinen in der Regel in chronologischer Reihenfolge im Posteingang. Auf den ersten Blick werden Absender:innen, die Betreffzeilen, kurze Auszüge aus den E-Mails und jeweils das Empfangsdatum angezeigt. Ein Klick mit der Maus auf die entsprechende E-Mail öffnet diese und zeigt dann den vollständigen Text an.

Der **Speicher** des E-Mail-Postfachs ist begrenzt. Ist es voll, können keine neuen E-Mails mehr empfangen werden, bis alte Nachrichten gelöscht sind. Insbesondere wenn oft Bilder verschickt und empfangen werden, sollte auf ausreichenden Speicherplatz geachtet und nicht mehr benötigte E-Mails regelmäßig gelöscht werden. Beim Versand großer Datenmengen empfiehlt es sich, diese entweder vorab in einem ZIP-Ordner zu komprimieren oder einen Cloud-Dienst zu verwenden und nur einen Link per E-Mail zu versenden.

ZIP (von englisch: zipper, auf Deutsch: Reißverschluss) ist ein Dateiformat, in dem digitale Daten verdichtet beziehungsweise reduziert werden und so weniger Speicherplatz und Übertragungszeit benötigen. So können auch ganze Ordner mit Unterordnern als eine Datei versendet werden. Persönliche oder sensible Dokumente können im ZIP-Dateiformat mit einem Passwort geschützt werden.

Webmail-Dienste haben den Vorteil, dass von jedem Computer mit Internetverbindung und mit jedem Webbrowser auf E-Mails zugegriffen werden kann. Der letzte Stand der Bearbeitung des Postfachs – also gelesene, verschobene, gelöschte E-Mails sowie das Adressbuch – ist dabei überall gleich: ob von zuhause, vom Computer im Vereinsbüro oder vom Urlaubsquartier aus. Der Nachteil ist, dass die Weboberflächen im Vergleich zu gängigen E-Mail-Programmen teilweise weniger Funktionen bieten und ohne Internetverbindung kein Zugriff auf bereits gelesenen E-Mails oder das Adressbuch besteht.

Hilfreiche Beiträge zu den eigenen Rechten im Bereich Internet und E-Mail stellt die Verbraucherzentrale bereit.
> vzbv.de/themen/digitale-welt

Wie mithilfe von Cloud-Anbietern online zusammengearbeitet werden kann, steht im digital verein(t)-Handbuch „Online-Zusammenarbeit: Projekte organisieren, erarbeiten und Wissen austauschen“.

Tipp 1 / E-Mail-Programm mit einem starken Passwort schützen.

Als E-Mail-Programm (auch E-Mail-Client genannt) wird ein auf dem PC, Laptop, Tablet oder Smartphone installiertes Programm bezeichnet, mit dem E-Mails empfangen und versendet werden. Mit E-Mail-Programmen kann auch ohne Internet auf das Postfach zugegriffen werden, allerdings ist der Abruf von anderen Geräten etwas komplizierter oder gar nicht möglich. Mit E-Mail-Programmen können in der Regel auch digitale Kalender, Notizen oder Aufgabenlisten erstellt und bearbeitet werden. Aufgrund des nicht zwingend erforderlichen Logins sollte bedacht werden, dass das Gerät mit dem E-Mail-Programm in falschen Händen auch unerwünschten Zugriff auf E-Mails und Adressbuch zur Folge haben kann. Die gängigsten E-Mail-Clients sind in Deutschland Microsoft Outlook, Mozilla Thunderbird und Apple Mail.

Opera Mail ist ein kostenloser E-Mail-Client mit vielfältigen Funktionen. Indem E-Mails hier in unterschiedlichen Tabs angelegt werden (ähnlich zu Browser-Tabs, die vom Surfen im Internet bekannt sein sollten), lassen sich Nachrichten übersichtlich verwalten. Opera Mail ist außerdem in der Lage, E-Mails nach zuvor festgelegten Regeln automatisch zu sortieren. Außerdem können unterschiedliche E-Mail-Accounts hinzugefügt und so parallel verwaltet werden.
> opera.com/de

Ein weiterer kostenloser E-Mail-Client ist **Pegasus Mail**. Auch hier lassen sich die E-Mails nach unterschiedlichen Kriterien sortieren und übersichtlich organisieren. Für das Verfassen von Nachrichten ist der eingebettete Rechtschreibprüfer Hunspell nützlich, der auf Fehler hinweist. Dank der SSL-Unterstützung können vertrauliche Nachrichten per SSL (Secure Socket Layer), einem Protokoll zur Verschlüsselung der Datenübertragung, verschlüsselt versendet werden.
> pmail.com/downloads_s3_t.htm

SeaMonkey ist mehr als ein Mail-Client, zum Beispiel sind ein Browser, Chatting-Client und weitere Hilfsprogramme vorhanden. Damit werden alle wichtigen Internetfunktionen in einem Tool zusammengeführt.
> seamonkey-project.org/releases

Der Mozilla-Client **Thunderbird** ist eine kostenlose Outlook-Alternative. Durch zahlreiche Add-ons kann das Programm individuell erweitert werden, unter anderem mit Modulen für die Termin- und Aufgabenverwaltung. Der Aufbau ist sehr übersichtlich und verfügt über oft genutzte Basisfunktionen.
> thunderbird.net/de

Tipp 2 / Bei größeren Rundmails die E-Mail-Versandoption BCC nutzen.

Für den Versand einer E-Mail an mehrere Adressen gibt es in jedem E-Mail-Programm drei Möglichkeiten:

„An“: Alle Adressen, die hier eingegeben werden, gelten als Hauptempfänger:innen der E-Mail. Alle Empfänger:innen können die hier angegebenen Adressen sehen.

„CC“: CC steht für „carbon copy“. Die Adressat:innen im CC-Feld gelten nicht als Hauptempfänger:innen, sie sollen die E-Mail nur zur Kenntnis nehmen. Auch die hier eingegebenen E-Mail-Adressen sind für alle Empfänger:innen sichtbar.

„BCC“: Nur im Feld „blind carbon copy“ sind die E-Mail-Adressen für die Empfänger:innen nicht sichtbar. Alle bekommen eine E-Mail, können aber nicht sehen, an wen die Rundmail sonst versendet wurde. Die Funktion BCC ist bei Rundmails wie Infoschreiben, Einladungen und Newsletter des Vereins **Pflicht**, wenn nicht absolut sicher ist, dass alle damit einverstanden sind, dass ihre E-Mail-Adressen einer größeren Runde mitgeteilt werden. In der Umsetzung kann die eigene E-Mail-Adresse ins Feld „An“ gesetzt werden (oder das Feld einfach leer lassen) und die restlichen Adressat:innen ins BCC-Feld setzen, dann bleibt die Liste anonym.

Tipp 3 / Sparsam mit der Angabe der eigenen und anderer E-Mail-Adressen umgehen.

Eine E-Mail-Adresse ist wie die Wohnadresse oder IBAN eine persönliche Information mit personenbezogenen Daten, die nur sparsam weitergegeben werden sollte. Sie kann auch anonymisiert werden. Wer sich vor Spam-Mails schützen möchte, muss sorgfältig mit seiner E-Mail-Adresse umgehen. Dabei helfen die folgenden Hinweise:

Spam (auf Deutsch: Müll) sind unerwünschte elektronische Nachrichten, die häufig Werbung enthalten. Meistens werden Spam-Mails vollautomatisch über spezielle Programme versandt. Im zweiten Kapitel wird der Frage nachgegangen, wie sich vor solchen Mails geschützt werden kann.

Die persönliche E-Mail-Adresse nicht wahllos in Online-Formulare eingeben: Wenn die E-Mail-Adresse bei Anmeldungen (etwa für Newsletter, Registrierungen, Bestellungen, Gewinnspiele) auf öffentlichen Plattformen oder in sozialen Netzwerken genutzt wird, landen innerhalb kurzer Zeit Spam-Mails im Postfach. Das liegt daran, dass Anbieter die Adressen an Werbetreibende weiterverkaufen, die dann unerwünschte E-Mails mit Werbung versenden. Darum verschiedene E-Mail-Adressen für unterschiedliche Dienste verwenden. Die Haupt-E-Mail-Adresse sollte nur an Personen weitergegeben werden, die Sie persönlich kennen.

Das BCC-Feld nutzen: Auch die E-Mail-Adressen anderer Personen können geschützt werden, wenn beim Versand von E-Mails an mehrere Personen die Adressen in das BCC-Feld geschrieben werden (mehr dazu oben unter den E-Mail-Versandoptionen).

Die „Antwort an"-Option auswählen: Sind mehrere Personen als Empfänger:innen einer E-Mail angegeben, kann bei der Antwort aus zwei Optionen gewählt werden: „Antwort nur an den Absender" oder „Antwort an alle". So bekommt entweder nur die Absenderadresse die Antwort-E-Mail oder alle, die in der Ursprungs-E-Mail als Empfänger:innen angegeben sind. Bei Verwechslung der Antwort-Option können nicht nur unangenehme Situationen entstehen, wenn beispielsweise eine vertrauliche Information an mehr Empfänger:innen geht als ursprünglich beabsichtigt. Antworten „an alle" überfüllen auch schnell die Postfächer der Emp- fänger:innen. Generell sollte beim Schreiben von E-Mails auf Informationen, die nicht unbedingt notwendig oder sensibel sind, verzichtet werden.

Weitergabe nur bei Einverständnis: E-Mail-Adressen dürfen nicht an andere Personen oder Organisationen weitergegeben werden, es sei denn, die Adressinhaber:innen sind damit ausdrücklich einverstanden, auch von diesen Personen oder Organisationen E-Mails zu bekommen.

Anonymisierung: Eine E-Mail-Adresse muss nicht unbedingt den eigenen Namen enthalten. Anne Meyer kann beispielsweise auch ein Namenskürzel verwenden wie AnMe@mail.de. Diese Form der Abkürzung schützt zwar nicht dauerhaft vor Spam, aber sie lässt keine Rückschlüsse zu, ob die Adresse einem Mann oder einer Frau gehört oder wie alt er oder sie sein könnte. Mit einem Pseudonym wie beispielsweise schneewittchen@mail. de ist die E-Mail-Adresse zwar komplett anonymisiert, könnte allerdings von den Kontakten als Spam eingeordnet werden. Daher genau abwägen, ob und wie die E-Mail-Adresse abgekürzt, anonymisiert oder pseudonymisiert wird.

Für die ehrenamtliche Arbeit oder im beruflichen Kontext sind E-Mail-Adressen mit echtem Vor- und Nachnamen ratsam. Das fördert Vertrauen und Transparenz. Sollte der gewünschte Name schon vergeben sein, können Vor- und Zuname durch Punkt oder Sonderzeichen getrennt werden. Zum Beispiel:

Erika.Mustermann@mustermail.de

Erika_Mustermann@mustermail.de

E.Mustermann@mustermail.de

Wenn der Verein eine eigene Website oder Domain hat, können E-Mail-Adressen mit dieser Domain erstellt werden. Für allgemeine Anfragen ist es sinnvoll, eine Infomail-Adresse nach dem Muster info@musterverein.de anzulegen. Im Impressum der eigenen Website oder eines Blogs empfiehlt sich, die E-Mail-Adresse mit ausgeschriebenen Satzzeichen und Klammern darzustellen: vorname(punkt)nachname(at)xxx(punkt) de. So kann die E-Mail-Adresse von einigen RoboterSoftwares nicht als E-Mail-Adresse erkannt und ausgelesen werden. Das schützt wirksam vor Spam.

Legen Sie eine E-Mail-Adresse für die persönliche, Vertrauen erfordernde Kommunikation, und eine zweite anonymisierte Adresse für Newsletter und Bestellungen an. Das kann bei der sicheren Nutzung von Plattformen und Onlineshops helfen.

Tipp 4 / Möglichst verschlüsselt kommunizieren.

E-Mails lassen sich mit Postkarten vergleichen, die auf dem Transportweg für alle lesbar sind, die berechtigt oder unberechtigt Zugriff darauf haben. Um Deine E-Mails vor fremden Blicken zu schützen, sollten sie verschlüsselt sein. Das ist insbesondere beim Versand von sensiblen Daten wichtig.

Es gibt zwei Verschlüsselungsmethoden: Die **Transportverschlüsselung** verschlüsselt jede E-Mail zwischen Absender:in und Empfänger:-in. Dabei liegt die E-Mail allerdings unverschlüsselt auf den Servern der E-Mail-Anbieter vor. Bei der **Ende-zu-Ende-Verschlüsselung** können dagegen nur Absender:in und Empfänger:in eine Nachricht lesen. Der E-Mail-Anbieter und andere Dritte haben keinen Zugriff auf die gesendeten Inhalte. Durch diese Art der Verschlüsselung wird aus einer normalen E-Mail ein Brief samt Umschlag.

Die Service DE-Mail wird auch von den deutschen Behörden akzeptiert

De-Mail ist ein E-Mail-Dienst, der elektronische Post inklusive angehängter Dokumente sicher und nachweisbar ermöglicht und daher auch von den deutschen Behörden akzeptiert wird. Die bekanntesten Anbieter von De-Mail-Adressen sind GMX, WEB.DE, Telekom und 1&1. De-Mail nutzt standardmäßig eine Transportverschlüsselung. Darüber hinaus gibt es die Möglichkeit, De-Mails mit einer Ende-zu-Ende-Verschlüsselung zu versenden.

Um die **Ende-zu-Ende-Verschlüsselung** zu nutzen, wird eine entsprechende Verschlüsselungssoftware benötigt. Die gängigsten Verschlüsselungsstandards sind PGP (Pretty Good Privacy) und S/MIME (Secure Multipurpose Internet Mail Extension). Während S/MIME vor allem in Behörden und Firmen genutzt wird, hat sich PGP eher im privaten Gebrauch durchgesetzt. Da die beiden Verschlüsselungsverfahren untereinander nicht kompatibel sind, müssen zwei Menschen, die miteinander verschlüsselt per E-Mail kommunizieren wollen, den gleichen Verschlüsselungsstandard verwenden.

Sowohl PGP als auch S/MIME nutzen das Prinzip der **asymmetrischen Kommunikation**, bei dem ein öffentlicher und ein privater Schlüssel zum Einsatz kommen. Der **öffentliche Schlüssel** ist öffentlich zugänglich. Er wird an die Kommunikationspartner:-innen verteilt. Mit diesem Schlüssel werden die E-Mails, die versendet werden sollen, verschlüsselt. Der **private Schlüssel** bleibt dagegen im eigenen Besitz.

Er darf mit niemandem geteilt werden und sollte so geheim bleiben wie die Daten beim Onlinebanking, denn der private Schlüssel entschlüsselt die verschlüsselten Nachrichten. Wer Personen anschreiben möchte, deren E-Mail-Konfigurationen keine Verschlüsselung unterstützen, kann Nachrichten weiterhin in unverschlüsselter Form senden. Eine Standardanleitung für alle E-Mail-Programme, Verschlüsselungsstandards und Betriebssysteme gibt es nicht. Falls eine E-Mail-Adresse von GMX oder WEB.DE genutzt wird, führt ein Assistent in drei Schritten von der Plug-in-Installation bis zur Schlüssel- und Passwort-Generierung. Aber auch in allen anderen Fällen ist es in der Regel mit nur wenigen Schritten möglich, andere Personen zur verschlüsselten Kommunikation einzuladen.

Im Internet sind mit den entsprechenden Suchbegriffen, Anleitungen zur Erstellung eines Schlüssels für die verschiedenen E-Mail-Programme und Betriebssysteme zu finden. Digital verein(t) stellt im Folgenden beispielhafte Anwendungen vor, mit denen E-Mails geschützt werden können. Alle aufgeführten Beispiele sind Open-Source-Programme. Das bedeutet, dass alle das Recht haben, sie kostenlos zu nutzen, und die Möglichkeit haben, den Quellcode der Programme zu untersuchen. So lässt sich die Vertrauenswürdigkeit der Programmierung und des Programms prüfen.

Für Nutzer:innen des E-Mail-Clients Mozilla Thunderbird steht das Plug-in **Enigmail** zur Verfügung. Mit Enigmail lassen sich sowohl der Nachrichtentext als auch die Betreffzeile verschlüsseln. Darüber hinaus werden auch Dateianhänge geschützt. Das Plug-in ist auch für den E-Mail-Dienst SeaMonkey verfügbar.
> enigmail.net/index.php/en

Gpg4win (GNU Privacy Guard for Windows) ist die gängigste Verschlüsselungssoftware zum Verschlüsseln und Signieren unter Windows. Mit Gpg4win kann jede E-Mail, jede Datei und jeder Datei-Ordner einfach und kostenlos ver- und entschlüsselt sowie die Integrität (Unveränderheit) und Herkunft (Authentizität) mittels digitaler Signaturen abgesichert und überprüft werden. Das Programm stellt zudem ein Handbuch zur Verfügung, in dem das Verschlüsseln von Nachrichten und Dateien in verständlichen Schritt-für-Schritt Anleitungen mit Bildern erklärt wird.
> gpg4win.org/index-de.html

Über die reine Verschlüsselung der E-Mail-Kommunikation hinaus kann es auch sinnvoll sein, einzelne Dateien oder ganze Ordner für den Versand zu verschlüsseln.

TruPax ist ein kostenloses Tool und sehr einfach zu handhaben. Es kann eine beliebige Auswahl von Dateien und Ordnern in Containerdateien verschlüsseln, die sich durch ein Passwort wieder entschlüsseln lassen.
> coderslagoon.com

2

Spam & Phishing

2

Spam & Phishing: Schutz vor schädlichen E-Mails

Sie haben ein großes Vermögen von einem reichen Prinzen am anderen Ende der Welt gewonnen, oder das Vereinskonto wurde angeblich gesperrt – manche E-Mails lösen gleich nach ihrem Erscheinen im Posteingang Unsicherheit aus. Woran sind schädliche E-Mails zu erkennen? Was bedeuten Spam und Phishing? Und wie gelingt der Schutz vor unerwünschten E-Mails? Um über das eigene Postfach die Kontrolle zu behalten, sollten einige grundlegende Verhaltensregeln berücksichtigt werden. Digital verein(t) zeigt in diesem Kapitel, wie es geht.

Tipp 5 / **E-Mails ungeöffnet löschen, wenn sie unseriös erscheinen und die Absender:innen unbekannt sind.**

Spam sind unerwünschte Nachrichten, die massenhaft per E-Mail oder über andere Kommunikationsdienste versendet werden. Es gibt verschiedene Arten von Spam-Mails. Dazu gehören unerwünschte Werbeangebote für bestimmte Onlineshops oder Produkte. Diese Art von Spam ist zwar lästig, aber kaum gefährlich. Es ist vergleichbar mit Werbebroschüren, die häufig im Briefkasten zu finden sind. Im Netz sind jedoch auch viele Spam-Mails im Umlauf, die ebenfalls einen werbenden Charakter haben können, hinter denen sich aber Betrugsversuche verbergen. Dabei werden Spam-Mails eingesetzt, um verschiedene Schadprogramme auf den Rechnern von E-Mail-Nutzer:innen zu installieren.

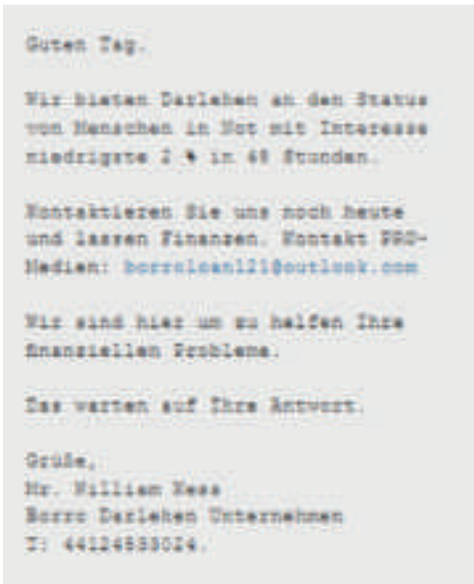
Bei Unsicherheiten, ob eine E-Mail seriös ist, kann die/der Absender:in im Internet recherchiert werden. Im Zweifelsfall aber gilt:

Solche E-Mails sofort und ungeöffnet löschen.

Niemals auf darin enthaltene Links klicken.

Keine Anhänge öffnen und diese auch nicht herunterladen.

Ein Betrugsversuch per E-Mail kann beispielsweise so aussehen:


Guten Tag.

Wir bieten Darlehen an den Status von Menschen in Not mit Interesse niedrigste 2 % in 48 Stunden.

Kontaktieren Sie uns noch heute und lassen Finanzen. Kontakt PRO-Medien: borrowloan121@outlook.com

Wir sind hier um zu helfen Ihre finanziellen Probleme.

Das warten auf Ihre Antwort.

Grüße,
Mr. William Rees
Borro Darlehen Unternehmen
T: 44124533014.

Nicht alle Betrüger:innen schreiben so offensichtlich fehlerhaft wie im obenstehenden Beispiel. Immer häufiger wirken E-Mails, die angeblich von Versandhäusern, der Post oder Banken verschickt wurden, täuschend echt. Hier empfehlen sich die folgenden Überprüfungsmethoden:

Die eventuell angegebene Website auf Plausibilität prüfen. Kann die Webadresse tatsächlich von dem Unternehmen stammen, von dem die Nachricht verschickt worden sein soll?

Telefonisch oder schriftlich nachfragen, ob die E-Mail mit der Forderung aus dem jeweiligen Unternehmen kommt oder nicht. **Keinesfalls** per Ant- worten-Button **auf die vermeintliche Spam-E-Mail antworten.**

Wenn noch Zweifel bestehen, die verdächtige E-Mail an das Unternehmen weiterleiten, von dem sie angeblich stammt. Dabei aber niemals auf Links in der E-Mail klicken und keine Anhänge öffnen.

Phishing setzt sich aus den englischen Wörtern „password“ und „fishing“ zusammen und bedeutet wörtlich übersetzt das Fischen nach Passwörtern. Dabei sollen die Empfänger:innen durch häufig sehr echt wirkende E-Mails dazu gebracht werden, auf einen Link zu klicken und auf der ebenfalls gefälschten Zielseite Passwörter beziehungsweise persönliche Daten einzugeben, die von Kriminellen abgegriffen und missbraucht werden.

Spam-Mails werden häufig für **Phishing-Angriffe** genutzt. Bei Phishing-Mails handeln die Betrüger:innen oft im Namen von vertrauenswürdigen Seiten wie Internetseiten von Banken. Auf gefälschten Seiten wird dazu aufgefordert, Log-in-Daten, PINs und TANs für das Onlinebanking einzugeben, Passwörter zu ändern oder persönliche Daten zu aktualisieren. Diese Daten werden an Kriminelle weitergeleitet, die sich damit auf der originalen Seite der Bank Zugang zum Konto verschaffen können.

Phishing-Mails können häufig an den folgenden Merkmalen erkannt werden:

Unpersönliche Anrede: Der eigene Name wird nicht genannt, zum Beispiel „Lieber Kunde des Unternehmens xy!“

Sprache: Manchmal sind die Nachrichten in fehlerhaftem Deutsch verfasst. Das ist so, weil sie von Computerprogrammen automatisch aus anderen Sprachen übersetzt werden.

Falsche Umlaute: Die E-Mails enthalten kyrillische Buchstaben oder falsch aufgelöste beziehungsweise fehlende Umlaute, zum Beispiel nur „a“ statt „ä“ beziehungsweise „ae“.

Nicht jede Phishing-Mail weist diese Merkmale auf, denn Phishing-Mails werden immer professioneller und persönlicher. Das sind weitere Erkennungsmerkmale:

Dringlichkeit: Es soll schnell auf irgendetwas reagiert werden, zum Beispiel „Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren …“.

Drohungen: Drastische Folgen werden angekündigt, zum Beispiel „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …“.

Abfrage vertraulicher Daten: Beispielsweise werden über ein Formular oder in der E-Mail nach PINs und TANs oder anderen vertraulichen Daten gefragt.

Gefälschte Absenderadresse: Die Absenderadresse wirkt auf den ersten Blick echt, enthält aber häufig noch zusätzliche Buchstaben, die keinen Sinn ergeben.

Links zu gefälschten Websites: In der Adresszeile erscheinen Internetadressen, die den echten ähnlich sind, aber unübliche Zusätze enthalten.

Auch wenn Phishing-Websites täuschend echt aussehen, gibt es neben den gefälschten Internetadressen weitere Hinweise, an denen sich die Fälschung erkennen lässt:

Fehlendes Sicherheitszertifikat: Das Sicherheitszertifikat einer Website sorgt für eine verschlüsselte Verbindung. Du kannst es an dem Schlosssymbol in der Statusleiste erkennen. Bei Phishing-Websites fehlt häufig dieses Schlosssymbol. Allerdings kann in manchen Fällen auch das gefälscht werden.

Falsches Kürzel: Die verschlüsselte Verbindung sind auch an der Adresszeile des Browsers mit dem Kürzel „https://“ zu erkennen. Fehlt das „s“ in dem Kürzel, dann ist die Website nicht verschlüsselt.

Datenabfrage: Auf der Anmeldeseite werden sensible persönliche Daten abgefragt, was seriöse Banken niemals machen würden.

Zur Übung: Auf der Seite des BSI für Bürger einige Beispiele für gefälschte Banken-Websites anschauen. Dafür können oben rechts in das Suchfeld die Begriffe „Beispiele Phishing-Angriffe“ eingegeben werden. Welche Details geben Hinweise auf eine unseriöse Website?
> bsi-fuer-buerger.de

Unterschiedliche Arten von Maleware

Tipp 6 / Den eigenen Rechner regelmäßig auf Schadprogramme prüfen.

Mit Schadprogrammen, sogenannter Malware, dringen Betrüger:innen in Computersysteme ein. Einmal infiziert, kann es unter anderem zu Datenverlust und -diebstahl, zu Hardware-Ausfällen oder gar zur Übernahme der Computersteuerung führen.

Malware leitet sich aus den englischen Wörtern „malicious“ (auf Deutsch: bösartig) und „software“ ab und steht für eine Vielzahl schädlicher Computerprogramme. Neben Viren, dem bekanntesten Beispiel für solche Schadprogramme, zählen unter anderem Spyware und Ransomware dazu. Während Spyware die Computeraktivitäten der Nutzer:innen überwacht und so an sensible Daten gelangt, fordert Ransomware ein Lösegeld für gesperrte Dateien oder das ganze Betriebssystem.

Folgende Maßnahmen können vor schädlichen Programmen schützen:

- Aktuelle Service-Packs und Sicherheitsupdates für das Betriebssystem installieren und automatische Updates aktivieren.
- Den Internetbrowser und die darin eingebundenen Plug-ins regelmäßig auf Aktualität prüfen.
- Einen Virenscanner installieren und diesen regelmäßig aktualisieren.
- Eine Firewall installieren.

In der Regel passiert eine Infizierung mit Schadprogrammen, ohne dass Nutzer:innen dies bemerken. Das kann zum Beispiel der Fall sein, wenn Dateien aus dem Internet heruntergeladen werden, die versteckte Malware enthalten. Darum ist es wichtig, den Rechner regelmäßig auf schädliche Programme zu überprüfen. Dafür gibt es praktische Tools, die den Rechner nicht nur auf Schadprogramme durchsuchen, sondern auch gefundene Schädlinge vom Rechner entfernen.

Tipp 7 / Einen Spam-Filter einrichten.

Profis können auf das kostenlose Open-Source-Programm **WireShark** zurückgreifen. Es wird für die Analyse von Netzwerken eingesetzt, indem es den Datenverkehr auf dem Computer überwacht. Ziel von WireShark ist es, unerlaubte Zugriffe aus dem Internet zu identifizieren. Für die Analyse der zahlreichen Daten, die bei der Überwachung des Netzwerks gesammelt werden, ist ein grundlegendes Verständnis über Netzwerkprotokolle empfehlenswert. Nur so lassen sich die Daten zielgerichtet auswerten und schädliche Programme identifizieren.
> wireshark.org

Mehr zu Sicherheitsupdates, Plug-Ins, Virenscanner und Firewall sind im digital verein(t)-Handbuch „Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen“ nachzulesen.

Jedes E-Mail-Konto bietet einen sogenannten Spam Filter zum Schutz vor Spam und Phishing. Dort landen E-Mails automatisch, wenn sie an einen Verteiler mit einer sehr großen Anzahl von E-Mail-Adressen gesendet wurden oder aus anderen Gründen verdächtig erscheinen. Es kann vorkommen, dass auch eine sichere E-Mail in den Spam-Ordner gelangt. Daher sollte ab und zu nachgeschaut werden, ob nicht auch eine wichtige Nachricht dort versehentlich gelandet ist. Viele Anbieter senden regelmäßige Spam-Berichte an die E-Mail-Adressen ihrer Nutzer:innen, die im normalen Posteingang landen. Damit lässt sich überprüfen, ob seriöse E-Mails versehentlich in den Filter gelangt sind. Die Einstellungen des Spam-Filters befinden sich in den Einstellungsoptionen des Webdienstes.

Die **Robinsonlisten** der Verbraucherschutzvereine und Verbände der Werbewirtschaft sind Listen, in die sich jede:r mit ihren/seien Kontaktdaten (von Faxnummer bis E-Mail-Adresse) eintragen kann, wenn keine Werbung erwünscht ist. Unternehmen haben Zugriff auf die Liste und können die eingetragenen E-Mail-Adressen aus ihrer Datenbank löschen.
> robinsonliste.de

Vielleicht wurde die eigene E-Mail-Adresse bereits im Internet veröffentlicht und könnte für kriminelle Zwecke verwendet werden. Das kann mit dem **Identity Leak Checker** vom Hasso-Plattner-Institut überprüft werden.
> sec.hpi.de/ilc

3

Messaging & Videotelefonie

3

Messaging & Videotelefonie: Zuverlässig verständigen – in Echtzeit

Vereinskommunikation findet zunehmend digital statt. Gerade wenn Vorstandsmitglieder sich schnell einmal austauschen müssen oder eine Terminfindung ansteht, sind Messenger-Dienste häufig die erste Wahl. Doch was sind Messenger-Dienste eigentlich? Wo spielt bei der sofortigen Nachrichtenübermittlung Privatsphäre eine Rolle? Und wie wird ein Videotelefonat durchgeführt? Um Messenger-Dienste guten Gewissens nutzen zu können, sollten vor allem die richtigen Sicherheitseinstellungen vorgenommen werden. Digital verein(t) zeigt in diesem Kapitel, wie das geht.

So funktionieren Messenger-Dienste

Mit Instant Messaging (auf Deutsch: sofortige Nachrichtenübermittlung) werden Nachrichten nahezu in Echtzeit ausgetauscht und es ist ein Gesprächsverlauf auf einem Blick in einem Fenster auf dem Bildschirm des Smartphones, Computers oder Tablets zu sehen. Neben reinen Textmitteilungen können auch Sprachnachrichten sowie Fotos, Videos und Dokumente versendet werden.

Die meisten Messenger-Dienste sind kostenfrei. Die entsprechende Software muss heruntergeladen und auf dem Gerät installiert werden. Dann können über die App Nachrichten an andere Personen gesendet werden, die ebenfalls diesen Messenger nutzen. Der Nachrichtenversand über das Internet ist kostenfrei, es wird jedoch Datenvolumen angerechnet. Der am weitesten verbreitete Messenger-Dienst ist in Deutschland nach einer Bitkom-Umfrage im Mai 2021 WhatsApp. Daneben gibt es besonders datensparsame Alternativen wie Wire, Threema und Signal, die weniger Daten erheben und speichern. (bitkom.org/Presse/Presseinformation/Auf-fast-jedem-Smartphone-wird-ein-Messenger-genutzt)

Tipp 8 / **Zugriffe und Funktionen der Messenger-Dienste prüfen.**

Inhalte werden nur zwischen Empfänger:innen und Sender:innen ausgetauscht. Für eine datensparsame und sichere Nutzung sollte bei der Auswahl des Messengers auf folgende Merkmale geachtet werden:

Ende-zu-Ende-Verschlüsselung: Diese Verschlüsselung sorgt dafür, dass Nachrichten auf dem Transportweg unlesbar bleiben und auch der Messenger-Anbieter die Kommunikationsinhalte nicht einsehen kann. Die meisten Messenger-Dienste bieten standardmäßig eine Ende-zu-Ende-Verschlüsselung an. Bei dem Messenger Telegram, eine beliebte Alternative zu WhatsApp, muss die Ende-zu-Ende-Verschlüsselung selbst in sogenannten „privaten Chats“ aktiviert werden. Bei Gruppenchats ist das allerdings nicht möglich.

Zugriff auf das Adressbuch: Einige Messenger wie WhatsApp synchronisieren die Adressbücher der Smartphones, auf denen sie installiert werden. Das erleichtert zwar die Kontaktaufnahme, dadurch haben aber auch die Betreiber der Messenger Zugriff auf das Telefonbuch. Wenn ein Messenger im Vereinskontext genutzt werden soll, wird dafür die Einwilligung der betroffenen Personen benötigt.

Speicherung von Metadaten: Bei der Nutzung von Messengern fallen sogenannte Metadaten an, die viel über die eigene Person und das persönliche Nutzungsverhalten aussagen, unter anderem wann jemand online ist oder wann mit wem kommuniziert wurde.

Der Messenger-Dienst WhatsApp behält sich beispielsweise in den Nutzungsbedingungen das Recht vor, diese Metadaten zu speichern, zu verwenden und zu teilen. Alternative Anbieter werben für mehr Datensparsamkeit und Privatsphäre und verzichten weitgehend auf die Speicherung dieser Daten.

Nutzungsbeschränkungen: Mit der Nutzung eines Messengers wird den jeweiligen Nutzungsbedingungen zugestimmt. Deshalb sollte sich mit diesen vertraut gemacht werden, damit mit der Verwendung nicht dagegen verstoßen wird. Der Messenger **WhatsApp darf beispielsweise nur privat genutzt werden**. Das bedeutet: Eine offizielle Nutzung im Vereinskontext verstößt gegen dessen Nutzungsbedingungen und ist nicht mit den Anforderungen der Europäischen Datenschutzgrundverordnung (kurz: DSGVO) an Organisationen vereinbar.

Blockieren unerwünschter Kontakte: Vorab oder spätestens, wenn es zu einer unerwünschten Kontaktaufnahme kommt, sollten Personen geblockt werden können. Eine Meldefunktion hilft bei Betrugsversuchen oder Cybermobbing.

Messenger-Dienste bieten die Möglichkeit Gruppen anzulegen. Zugang haben hier jene Personen, die von den Gruppenverwaltenden (sogenannte Admins) als Teilnehmende eingeladen werden. Solche Gruppenchats sollten immer mit Bedacht erstellt und geführt werden, da sich die Zahl der Teilnehmenden und damit auch der versendeten Nachrichten schnell erhöhen kann. Bei manchen Messenger-Diensten sehen Mitglieder eines Gruppenchats persönliche Daten wie die Telefonnummer und das Profilbild. Darum sollte bei der Nutzung bewusst mit der Privatsphäre umgegangen werden. Bevor im Verein eine solche Chatgruppe eingerichtet wird (beispielsweise für den Vorstand oder eine Mannschaft), ist es ratsam, mit allen geplanten Gruppenmitgliedern darüber zu sprechen.

Tipp 9

Beim Instant Messaging auf Datensparsamkeit und Privatsphäre achten.

Durch folgende Maßnahmen kann die Privatsphäre bei der Nutzung von Messenger-Diensten geschützt werden:

Den Nutzernamen **verkürzen oder anonymisieren.** In den meisten Fällen lassen sich die Profilangaben über die Messenger-Einstellungen nachträglich noch beliebig ändern.

Beim **Profilfoto** möglichst darauf achten, dass wenig von sich selbst zu erkennen ist.

Den **Online-Status** ausschalten. Dieser wird nicht nur im Messenger selbst, sondern auch auf der öffentlichen Profilseite im Internet angezeigt und ist somit nicht nur für bestätigte Kontakte, sondern auch für beliebige Personen sichtbar.

Nur Personen in die **Kontakte aufnehmen**, die aus anderen Kontexten bekannt sind.

Nachrichten sowie Anfragen für Dateiversand, Webcam- („Cam“) und Telefonfunktionen („Voice“) von **Unbekannten** generell ablehnen. Auch diese Funktion kann in den Privatsphäre-Einstellungen vorgenommen werden.

Keine sehr **privaten Bilder** oder wichtige **Daten** wie Passwörter, Bankdaten oder Kreditkartennummern versenden.

Ausführlichere Informationen zu datensparsamen Messenger-Diensten sind bei der Verbraucherzentrale in dem Artikel „WhatsApp- Alternativen: die Datenschutzregeln im Überblick“ zu finden. Dazu in das Suchfeld die Begriffe „WhatsApp-Alternativen“ eingeben.
> verbraucherzentrale.de

Zur Übung: Welcher Dienst kann aus welchen Gründen vorgezogen werden? Um hierfür eine Antwort zu finden, können Sie die Privatsphäre-Optionen und die Verschlüsselungsstandards Ihrer zwei favorisierten Messenger-Dienste recherchieren und miteinander vergleichen.

Tipp 10

Bei Video-Anrufen auf die Sicherheitseinstellungen des Dienstes und auf die Privatsphäre achten.

Videoanrufe sind eine weitere Funktion von Messenger-Diensten und in der Regel kostenfrei nutzbar. Heutige Smartphones, Tablets und Computer verfügen zumeist standardmäßig über die dafür benötigte Videokamera (Webcam) und das Mikrofon.

Die Sicherheit bei der Videotelefonie hängt von der Sicherheit des benutzten Geräts ab. Daher ist es ratsam, zunächst zu prüfen, ob Virenschutz, Firewall, Browser und Router aktuell sind. Danach sind die die Privatsphäre-Einstellungen in den Programmen selbst an der Reihe, welche manuell angepasst werden sollten. Hier kann unter anderem ausgewählt werden, wer über das Programm Kontakt aufnehmen darf.

Zum weiteren Schutz der eigenen Privatsphäre sind die folgenden Maßnahmen empfehlenswert:

Keine privaten Bilder oder Informationen mit unbekannten Personen teilen.

Darauf achten, was im Bild zu sehen ist. Große Teile der Umgebung wie zum Beispiel das Büro, die Wohnung oder der Urlaubsort können Informationen für eine rechtswidrige Nutzung liefern.

Immer ausloggen. Kriminelle könnten über ein laufendes Programm auch auf andere Programme zugreifen, die parallel zum Videochat geöffnet sind, sogar auf die Kamera. Wenn die Kamera nicht genutzt wird, diese mit einem Stück Klebezettel abkleben, damit sie nicht per Fernzugriff genutzt werden kann.

Sich bewusst machen, dass das Gegenüber eines **Videoanrufes Mitschnitte** der Gespräche erstellen kann. Solche gespeicherten Videos können unter anderem zu Mobbing-Zwecken missbraucht werden.

Weitere Informationen zum Thema Cybermobbing sind im digital verein(t)-Handbuch „Soziale Netzwerke: Kennenlernen, nutzen und souverän kommunizieren“ zu finden.

Funktionen von Videotelefonie-Diensten

Ein sehr bekannter Messenger-Dienst für Videotelefonie ist Skype. Daneben sind FaceTime, Google Hangouts sowie WhatsApp häufig genutzte Programme für Videotelefonie. Bei der Auswahl kann man sich daran orientieren, welchen Dienst die anderen Vereinsmitglieder und der Freundeskreis nutzen – unter Berücksichtigung der Alternativen.

Die bekanntesten Messenger-Dienste für Videotelefonie (links) und besonders datensparsame Alternativen (links)

Qualitativ und aus technischer Sicht gibt es bei den Angeboten keine großen Unterschiede, Voraussetzung ist allerdings ein ausreichend schneller Internetzugang. Das kann beispielsweise unter > speedtest.t-online.de getestet werden. Die wichtigsten Funktionen der Videotelefonie sind:

- Adressbuch;
- Chat-Funktion (bei schlechter Internet-Verbindung kann auf Textkommunikation ausgewichen werden);
- Lautstärke-Einstellungen;
- Ausblenden der Bildaufnahme (falls während des Gesprächs kurzzeitig etwas nicht gesehen werden soll, kann die Bildübertragung unterbrochen werden).

Auch bei der Anmeldung für Videotelefonie-Programme sollte auf Datensparsamkeit geachtet und nur die persönlichen Daten eingegeben werden, die für die Nutzung des Programms wirklich benötigt werden.

Zur Übung: Welches Videotelefonie-Programm kommt für Ihre Zwecke in Frage? Welche Probleme könnten sich durch die Videoübertragung ergeben? Welche Möglichkeiten haben Nutzer:innen, ihre Privatsphäre bei der Videotelefonie zu schützen? Ist nach Betrachtung dieser Fragestellungen der ausgewählte Dienst immer noch die beste Wahl?

Platz für Notizen

Checkliste

10 Tipps: Online kommunizieren – aber sicher!

- **Tipp 1**
  E-Mail-Programm mit einem starken Passwort schützen.
- **Tipp 2**
  Bei größeren Rundmails die E-Mail-Versandoption BCC nutzen.
- **Tipp 3**
  Sparsam mit der Angabe der eigenen und anderer E-Mail-Adressen umgehen.
- **Tipp 4**
  Möglichst verschlüsselt kommunizieren.
- **Tipp 5**
  E-Mails ungeöffnet löschen, wenn sie unseriös erscheinen und die Absender:innen unbekannt sind.
- **Tipp 6**
  Den eigenen Rechner regelmäßig auf Schadprogramme prüfen.
- **Tipp 7**
  Einen Spam-Filter einrichten.
- **Tipp 8**
  Zugriffe und Funktionen der Messenger-Dienste prüfen.
- **Tipp 9**
  Beim Instant Messaging auf Datensparsamkeit und Privatsphäre achten.
- **Tipp 10**
  Bei Video-Anrufen auf die Sicherheitseinstellungen des Dienstes und auf die Privatsphäre achten.

Weitere Themen und Informationen unter:
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.
> 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 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.
> sicher-im-netz.de

lagfa bayern

Die **lagfa bayern** versteht sich als Brückenbauer zwischen Zivilgesellschaft, Staat und Wirtschaft und handelt bedarfsorientiert als Partner und Berater 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.
> lagfa-bayern.de

Digitale Nachbarschaft

Mit der **Digitalen Nachbarschaft (DiNa)** sensibilisiert Deutschland sicher im Netz e.V. Vereine, Initiativen und freiwillig engagierte Bürger:innen für die Chancen der Digitalisierung. Die DiNa wird in Kooperation mit dem Bundesnetzwerk Bürgerschaftliches Engagement (BBE) durchgeführt. Gefördert wird das Projekt durch das Bundesministerium des Innern, für Bau und Heimat, unterstützt von der Deutschen Telekom AG, Huawei Technologies Deutschland GmbH und der Deutschen Bahn AG.
> digitale-nachbarschaft.de

Mehr digitale Themen

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

Laden Sie kostenlos die SiBa-App herunter:
> 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.
> sicher-im-netz.de/dsin-computercheck

Sie möchten 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 **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.
> 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.
> 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.
> 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.
> 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.
> so-geht-digital.de

Die neue **browserbasierte Simon-App** klärt über digitale Sicherheit im Alltag auf. Sie bietet Schutz- und Sicherheitswissen in leicht verständlichen Themenbereichen. Ein Quiz motiviert dazu, die eigenen digitalen Kompetenzen zu testen und Wissenslücken zu schließen. Über die Soforthilfe erhalten Nutzer:innen Schritt-für-Schritt-Anleitungen zur Selbsthilfe bei den häufigsten Schadensfällen im Internet.
> simon-app.org

Digital verein(t) vor Ort

digital verein(t)

digital verein(t)
lagfa bayern e.V.
Konrad-Adenauer-Allee 43
86150 Augsburg
Tel. 0821/20 71 48-15
digital-vereint.de

@digitalvereint

@digitalvereint

Machen Sie mit
im Verein!

Ehrenamtsagentur
„Aschaffenburg aktiv!"
Aschaffenburg

Freiwilligen-Zentrum
Bayreuth

Freiwilligenagentur
Landkreis Berchtesgadener Land

Koordinierungszentrum
Bürgerschaftliches Engagement
„Treffpunkt Ehrenamt"
Landkreis Cham

Ehrenamtsbüro
Landkreis Erlangen-Höchstadt

Freiwilligen-Zentrum „auf geht's"
Garmisch-Partenkirchen

Freiwilligenagentur
Mehrgenerationenhaus
Haßfurt

Koordinierungszentrum
Bürgerschaftliches Engagement
Landkreis Kulmbach

Freiwilligenagentur „fala"
Landshut

Freiwilligenangentur
Schaffenslust Memmingen
und Landkreis Unterallgäu

Förderstelle für
Bürgerschaftliches Engagement
„FöBE" München

Koordinierungszentrum
Bürgerschaftliches Engagement
Landkreis Neuburg-Schroben-
hausen

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

Freiwilligenagentur
Landkreis Oberallgäu

Servicestelle EhrenAmt
Landkreis Ostallgäu

ARBERLAND REGio
Landkreis Regen

Koordinierungszentrum
Bürgerschaftliches
Engagement
Freiwilligenagentur
Landkreis Regensburg

Freiwilligenagentur
„pack ma's"
Landkreis Rottal-Inn

Servicestelle Ehrenamt
Landkreis Schweinfurt

Koordinierungszentrum
Bürgerschaftliches ENgagement
Landkreis Wunsiedel

Servicestelle Ehrenamt
Landkreis Würzburg