Dein Verein tauscht sich aus

Digitale Nachbarschaft

Online-Kommunikation: Mailen, Messenger nutzen und Videoanrufe starten

Impressum

Redaktion: Dr. Elisabeth Maria Hofmann, Daniel Helmes (BBE), Petra Rollfing
Gestaltung und Satz: wegewerk GmbH
Erscheinungsjahr: 2019
3., durchgesehene und aktualisierte Auflage 2021: 1.000

Herausgeber: Deutschland sicher im Netz e.V.
Projekt Nachbarschaft Digital >Ehrenamt >Sicher >Transformieren
Leitung: Dr. Nils Weichert
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

Online-Kommunikation: Mailen, Messenger nutzen und Videoanrufe starten

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 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 „blind carbon copy"-Funktion an eine größere Gruppe versendet werden, ohne dass alle E-Mail-Adressen für die einzelnen Empfänger*innen sichtbar sind. Auch die gemeinsame Vorstandssitzung in großen Einzugsgebieten profitiert von digitalen Werkzeugen. Nichts ersetzt den persönlichen Austausch. Aber wenn dieser aufgrund zu großer Entfernungen nur selten möglich ist, kann eine Videokonferenz zu viele E-Mails und einige Missverständnisse vermeiden. Das verbale Ping Pong via Videotelefonie gelingt mit wenig Vorbereitung und der Rücksicht auf einige Sicherheitsaspekte.

Die Digitale Nachbarschaft hat **10 DiNa-Tipps** formuliert, die Dir helfen, die digitalen Chancen für Dich und Deinen Verein sicher zu nutzen. Im ersten Kapitel geht es um die unterschiedlichen Möglichkeiten, E-Mails zu versenden. Im zweiten Kapitel erklären wir, wie Du Dich vor schädlichen E-Mails schützt. Und im dritten Kapitel erfährst Du, wie Du die unterschiedlichen Funktionen von Messenger-Diensten sicher nutzt.

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.

Webmail & E-Mail-Programme: Wie Du mit elektronischen Nachrichten zum Ziel kommst

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, solltest Du zu Beginn die richtigen Entscheidungen treffen. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

Die bekanntesten kostenfreien Webmail-Dienste (links) und besonders datensparsame Alternativen (rechts)

Webmail-Dienste und E-Mail-Programme

E-Mails sind elektronische Nachrichten, die neben Texten auch Bilder und andere Dateien enthalten können. 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.

Mache eine Liste der Kommunikationsaufgaben, die Du digital erledigen kannst. Gibt es vorinstallierte Kommunikations-Apps auf Deinem Smartphone? Welche davon würdest Du nutzen oder nutzt Du bereits 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 Nutzer*innendaten 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. Achte dabei auf Datensparsamkeit und gib nur die persönlichen Daten an, die für die E-Mail-Nutzung wirklich nötig sind.

Ausführlichere Informationen zum Umgang mit persönlichen und sensiblen Daten findest Du im DiNa-Handbuch „Mitgliederdaten: Schützen, verwalten und verwenden“ sowie in der multimedialen Reportage „Datenschutz und Sicherheit“ auf der Plattform ► https://dabei-geschichten.telekom.com/.

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 Du oft Bilder verschickst und empfängst, solltest Du auf ausreichenden Speicherplatz achten und nicht mehr benötigte E-Mails regelmäßig löschen. 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 kannst Du auch ganze Ordner mit Unterordnern als eine Datei versenden. Persönliche oder sensible Dokumente können im ZIP-Dateiformat mit einem Passwort geschützt werden.

Webmail-Dienste haben den Vorteil, dass Du von jedem Computer mit Internetverbindung und mit jedem Webbrowser auf Deine E-Mails zugreifen kannst. 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 Du ohne Internetverbindung keinen Zugriff auf Deine bereits gelesenen E-Mails oder das Adressbuch hast.

Hilfreiche Beiträge zu Deinen Rechten im Bereich Internet und E-Mail findest Du bei der Verbraucherzentrale. ► www.vzbv.de/themen/digitale-welt

Wie Du mithilfe von Cloud-Anbietern online zusammenarbeitest, erfährst Du im DiNa-Handbuch „Online-Zusammenarbeit: Projekte organisieren, erarbeiten und Wissen austauschen“.

DiNa-Tipp

DiNa-Tipp 1: Schütze Dein E-Mail-Programm mit einem starken Passwort!

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 kannst Du auch ohne Internet auf Dein Postfach zugreifen, 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 Log-ins 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 Du vom Surfen im Internet kennst), lassen sich Nachrichten übersichtlich verwalten. Opera Mail ist außerdem in der Lage, E-Mails nach zuvor festgelegten Regeln automatisch zu sortieren. Außerdem kön-

nen unterschiedliche E-Mail-Accounts hinzugefügt und so parallel verwaltet werden.
► www.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. ► www.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.
► www.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. ► www.thunderbird.net/de

DiNa-Tipp

DiNa-Tipp 2: Nutze bei größeren Rundmails die E-Mail-Versandoption BCC!

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 Empfänger*innen bekommen eine E-Mail, können aber nicht sehen, an wen die Rundmail sonst noch ging. Die Funktion BCC ist bei Rundmails wie beispielsweise Infoschreiben, Einladungen und Newsletter des Vereins Pflicht, wenn nicht absolut sicher ist, dass alle Empfänger*innen damit einverstanden sind, dass ihre E-Mail-Adressen einer größeren Runde mitgeteilt werden. Setze einfach Deine eigene E-Mail-Adresse ins Feld „An“ (oder lass das Feld einfach leer) und den Rest ins BCC-Feld, dann bleibt die Empfänger*innenliste anonym.

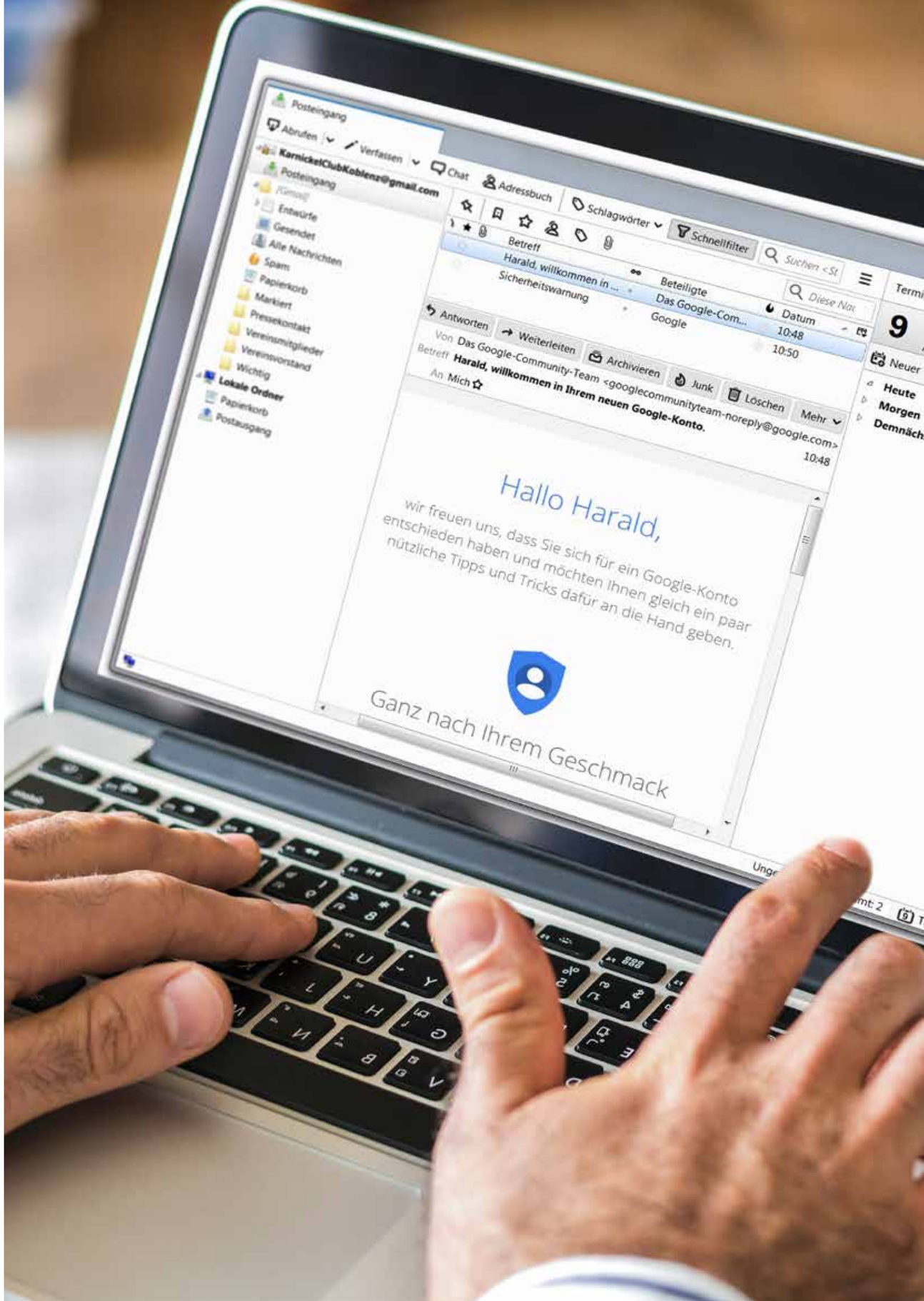
DiNa-Tipp

DiNa-Tipp 3: Gehe sparsam mit der Angabe Deiner und anderer E-Mail-Adressen um!

Eine E-Mail-Adresse ist wie die Wohnadresse oder Deine 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 erfährst Du, wie Du Dich vor solchen Mails schützt.

- **Gib Deine E-Mail-Adresse nicht wahllos in Online-Formulare ein:** 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 in Deinem Postfach. Das liegt daran, dass Anbieter die Adressen an Werbetreibende weiterverkaufen, die dann unerwünschte E-Mails mit Werbung senden. Nutze darum verschiedene E-Mail-Adressen für unterschiedliche Dienste. Deine Haupt-E-Mail-Adresse sollte nur an Personen weitergegeben werden, die Du persönlich kennst.



- **Nutze das BCC-Feld:** Auch die E-Mail-Adressen anderer können geschützt werden, wenn Du beim Versand von E-Mails an mehrere Empfänger*innen die Adressen in das BCC-Feld schreibst (mehr dazu oben unter den E-Mail-Versandoptionen).

- **Wähle die „Antwort an"-Option aus:** Sind mehrere Personen als Empfänger*innen einer E-Mail angegeben, die auch Du bekommen hast, kannst Du bei der Antwort aus zwei Optionen wählen: „Antwort nur an den Absender" oder „Antwort an alle". So bekommt entweder nur die Absenderadresse Deine 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 Empfänger*innen. Generell solltest Du beim Schreiben von E-Mails auf Informationen, die nicht unbedingt notwendig oder sensibel sind, verzichten.

- **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. Wäge daher ab, ob und wie Du Deine E-Mail-Adresse abkürzt, anonymisierst oder pseudonymisierst.

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 wie beispielsweise

- Erika.Mustermann@mustermail.de
- Erika_Mustermann@mustermail.de
- E.Mustermann@mustermail.de

Wenn Dein Verein eine eigene Website oder Domain hat, kannst Du E-Mail-Adressen mit dieser Domain erstellen. Für allgemeine Anfragen ist es sinnvoll, eine Infomail-Adresse nach dem Muster info@mustervereine.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 Roboter-Softwares nicht als E-Mail-Adresse erkannt und ausgelesen werden. Das schützt wirksam vor Spam.

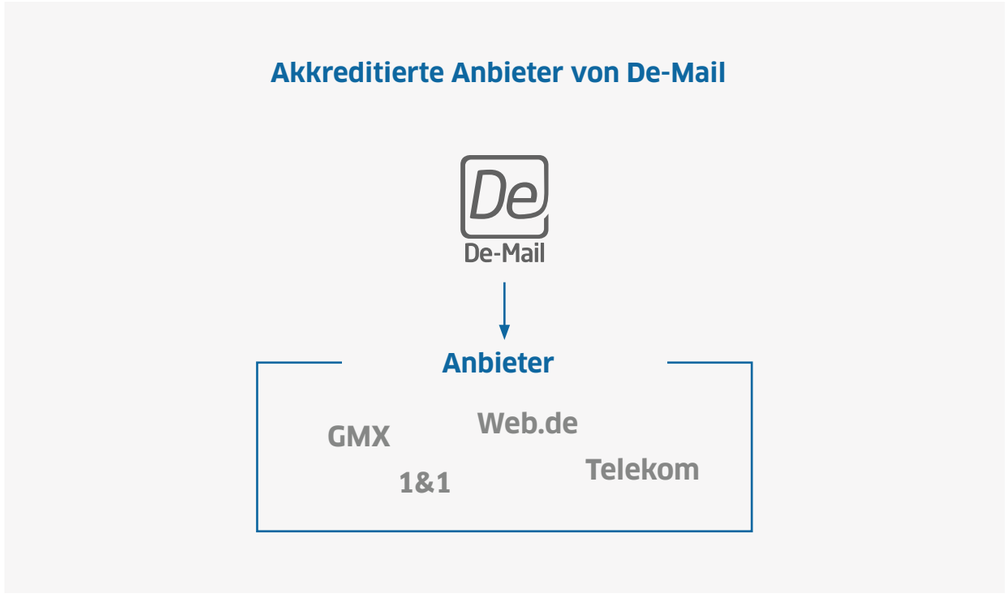
Lege Dir zwei E-Mail-Adressen an: Eine für die persönliche Kommunikation, die Vertrauen erfordert; und eine zweite, anonymisierte für Newsletter-Anmeldungen und Bestellungen.

DiNa-Tipp

DiNa-Tipp 4: Kommuniziere möglichst verschlüsselt!

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, solltest Du sie verschlüsseln. Das ist insbesondere beim Versand von sensiblen Daten wichtig.

Es gibt zwei Verschlüsselungsmethoden: Die **Transportverschlüsselung** verschlüsselt jede E-Mail bei der Übermittlung 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.



Der 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, benötigst Du eine entsprechende Verschlüsselungssoftware. 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 Empfänger*innen 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 Du eine E-Mail-Adresse von GMX oder WEB.DE nutzt, führt Dich ein Assistent in drei Schritten von der Plug-in-Installation bis zur Schlüssel- und Passwort-Generierung. Aber auch in allen anderen Fällen bist Du in der Regel nach nur wenigen Schritten in der Lage, Kommunikationspartner*innen zur verschlüsselten Kommunikation einzuladen.

Im Internet findest Du mit den entsprechenden Suchbegriffen Anleitungen zur Erstellung eines Schlüssels für die verschiedenen E-Mail-Programme und Betriebssysteme. Wir stellen im Folgenden beispielhafte Anwendungen vor, mit denen Du Deine E-Mails schützen kannst. Alle aufgeführten Beispiele sind Open-Source-Programme. Das bedeutet, dass jede*r das Recht hat, sie kostenlos zu nutzen, und die Möglichkeit besitzt, 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. ▸ www.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.
▸ www.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. ▸ www.coderslagoon.com

2

Spam & Phishing: Wie Du Dich vor schädlichen E-Mails schützt

Dein Verein hat ein großes Vermögen von einem Gönner am anderen Ende der Welt gewonnen, 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 kannst Du Dich vor unerwünschten E-Mails schützen? Um über Dein Postfach die Kontrolle zu behalten, solltest Du einige grundlegende Verhaltensregeln berücksichtigen. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

DiNa-Tipp

DiNa-Tipp 5: Lösche E-Mails ungeöffnet, wenn sie Dir unseriös erscheinen und Dir 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 ungewünschte Werbeangebote für bestimmte Onlineshops oder Produkte. Diese Art von Spam ist zwar lästig, aber kaum gefährlich. Es ist vergleichbar mit unerwünschten Werbebroschüren, die Du häufig in Deinem Briefkasten findest. 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.

Wenn Du nicht sicher bist, ob eine E-Mail seriös ist, kannst Du die/den Absender*in im Internet recherchieren. Im Zweifelsfall aber gilt:

- Lösche solche E-Mails sofort und ungeöffnet.
- Klicke niemals auf darin enthaltene Links.
- Öffne keine Anhänge und lade sie auch nicht herunter.

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: borroloan121@outlook.com

Wir sind hier um zu helfen Ihre
finanziellen Probleme.

Das warten auf Ihre Antwort.

Grüße,
Mr. William Kess
Borro Darlehen Unternehmen
T: 44124533024.
```

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

- Rufe die eventuell angegebene Website im Browser auf. Klick dazu nicht auf die Kontaktdaten- oder Webseitenlinks in der E-Mail, sondern gib die URL manuell in den Browser oder die Suchmaschine ein.
- Frage telefonisch oder schriftlich nach, ob die E-Mail mit der Forderung aus dem jeweiligen Unternehmen kommt oder nicht. Antworte keinesfalls auf die vermeintliche Spam-E-Mail.
- Wenn Du noch Zweifel hast, leite die verdächtige E-Mail an das Unternehmen weiter, von dem sie angeblich stammt. Klicke dabei aber niemals auf Links in der E-Mail und öffne keine Anhänge.

i

Phishing setzt sich aus den englischen Wörtern „password" und „fishing" zusammen und bedeutet wörtlich übersetzt das Fischen nach Passwörtern. Beim Phishing sollen Nutzer*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 Angreifer*innen abgegriffen und missbraucht werden.

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

- **Unpersönliche Anrede:** Dein 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".

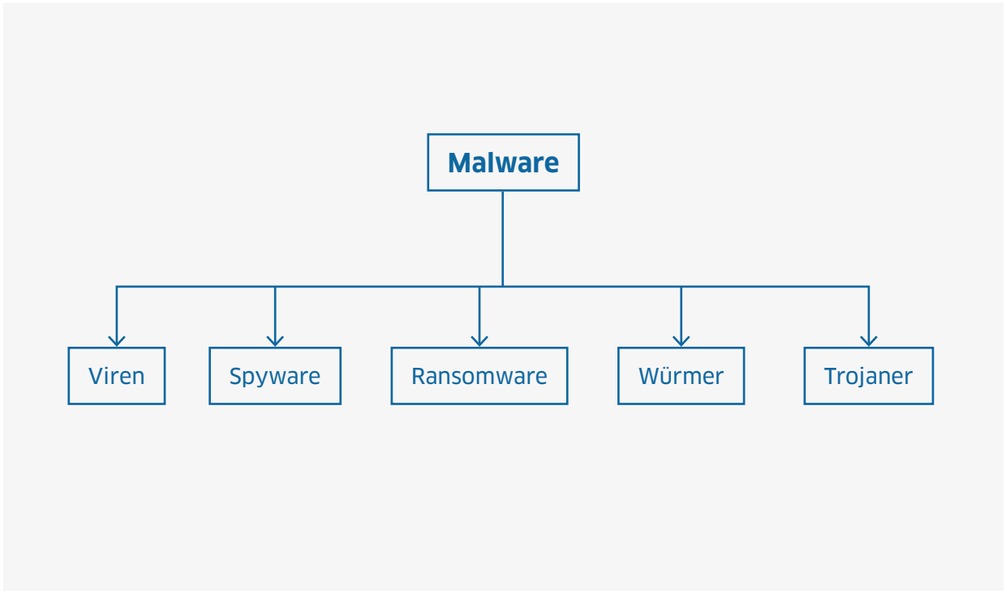
Nicht jede Phishing-Mail weist diese Merkmale auf, denn Phishing-Mails werden immer professioneller und persönlicher. Das sind weitere Erkennungsmerkmale:

- **Dringlichkeit:** Du sollst auf irgendetwas schnell reagieren, zum Beispiel „Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren …".
- **Drohungen:** Dir werden drastische Folgen angekündigt, zum Beispiel „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren …".
- **Abfrage vertraulicher Daten:** Du wirst beispielsweise über ein Formular oder in der E-Mail nach Deinen 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 erkennst Du auch an der Adresszeile des Browsers mit dem Kürzel „https://". 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.

Schau Dir auf der Seite des BSI für Bürger Beispiele für gefälschte Banken-Websites an. Welche Details geben Hinweise auf eine unseriöse Website? Die Beispiele findest Du, wenn Du auf ▸www.bsi-fuer-buerger.de oben rechts in das Suchfeld die Begriffe „Beispiele Phishing-Angriffe" eingibst.



Unterschiedliche Arten von Malware

DiNa-Tipp

DiNa-Tipp 6: Prüfe Deinen Rechner regelmäßig auf Schadprogramme!

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.

Mit den folgenden Maßnahmen schützt Du Dich vor schädlichen Programmen:

- Installiere aktuelle Service-Packs und Sicherheitsupdates für Dein Betriebssystem und aktiviere automatische Updates.
- Überprüfe Deinen Internetbrowser und die darin eingebundenen Plug-ins regelmäßig auf Aktualität.
- Installiere einen Virenscanner und aktualisiere diesen regelmäßig.
- Installiere eine Firewall.

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

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.
▸ www.wireshark.org

Mehr zu Sicherheitsupdates, Plug-Ins, Virenscanner und Firewall kannst Du im DiNa-Handbuch „Gemeinsam im Netz: Geräte absichern, Informationen sammeln und Netzwerke teilen" nachlesen.

DiNa-Tipp 7: Richte einen Spam-Filter ein!

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 solltest Du ab und zu nachschauen, 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 kannst Du in den Einstellungsoptionen des Webdienstes selbst vornehmen.

Die **Robinsonlisten** der Verbraucherschutzvereine und Verbände der Werbewirtschaft sind Listen, in die Du Dich mit Deinen Kontaktdaten (von Faxnummer bis E-Mail-Adresse) eintragen kannst, wenn Du keine Werbung wünschst. Registrierte Unternehmen haben Zugriff auf die Liste und können die eingetragenen E-Mail-Adressen aus ihrer Datenbank löschen.
▸ www.robinsonliste.de

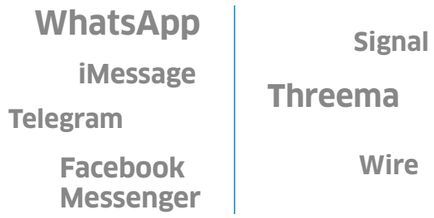
Vielleicht wurde Deine E-Mail-Adresse bereits im Internet veröffentlicht und könnte für kriminelle Zwecke verwendet werden. Das kannst Du mit dem **Identity Leak Checker** vom Hasso-Plattner-Institut überprüfen.
▸ www.sec.hpi.de/ilc

DiNa-Tipp

Messaging & Videotelefonie: Wie Du Dich in Echtzeit zuverlässig verständigst

Vereinskommunikation findet zunehmend digital statt. Gerade wenn Vorstandsmitglieder sich schnell einmal austauschen müssen oder eine Terminfindung ansteht, sind Messenger-Dienste häufig erste Wahl. Doch was sind Messenger-Dienste eigentlich? Wo spielt bei der sofortigen Nachrichtenübermittlung Privatsphäre eine Rolle? Und wie führst Du Videotelefonate? Um Messenger-Dienste guten Gewissens zu nutzen, solltest Du vor allem die richtigen Sicherheitseinstellungen vornehmen. Die Digitale Nachbarschaft zeigt Dir in diesem Kapitel, wie es geht.

So funktionieren Messenger-Dienste



Die verbreitetsten Messenger-Dienste (links) und besonders datensparsame Alternativen (rechts)

Mit **Instant Messaging** (auf Deutsch: sofortige Nachrichtenübermittlung) tauschst Du Nachrichten nahezu in Echtzeit aus und siehst dabei den Gesprächsverlauf auf einen Blick in einem Fenster auf dem Bildschirm Deines Smartphones, Computers oder Tablets. 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 Deinem 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. Die am weitesten verbreiteten Messenger-Dienste sind in Deutschland nach einer Bitkom-Umfrage WhatsApp, Facebook Messenger und iMessage. Daneben gibt es besonders datensparsame Alternativen wie Wire, Threema und Signal, die weniger Nutzer*innendaten erheben und speichern.

DiNa-Tipp 8: Prüfe Zugriffe und Funktionen Deiner Messenger-Dienste!

DiNa-Tipp

Im Gegensatz zu sozialen Netzwerken ist die Kommunikation per Messenger nicht öffentlich. Die Inhalte werden nur zwischen Empfänger*innen und Sender*innen ausgetauscht. Für eine datensparsame und sichere Nutzung solltest Du bei der Auswahl Deines Messengers auf folgende Merkmale achten:

- **Ende-zu-Ende-Verschlüsselung:** Diese Verschlüsselung sorgt dafür, dass Deine Nachrichten auf dem Transportweg unlesbar bleiben und auch der Messenger-Anbieter Deine 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, musst Du die Ende-zu-Ende-Verschlüsselung selbst in sogenannten „privaten Chats" aktivieren. 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 zwischen Nutzer*innen, dadurch haben aber auch die Betreiber der Messenger Zugriff auf Dein Telefonbuch. Wenn Du einen Messenger im Vereinskontext nutzt, dann brauchst Du dafür die Einwilligung der betroffenen Personen.

- **Speicherung von Metadaten:** Bei der Nutzung von Messengern fallen sogenannte Metadaten an, die viel über Dich und Dein Nutzungsverhalten aussagen, unter anderem wann Du online bist oder wann Du mit wem kommuniziert. 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 stimmst Du den jeweiligen Nutzungsbedingungen zu. Mache Dich mit diesen vertraut, damit Du mit der Verwendung nicht dagegen verstößt. Den Messenger WhatsApp darfst Du beispielsweise nur privat nutzen. 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 andere Teilnehmende eines Gruppenchats persönliche Daten von Dir wie Deine Telefonnummer und Dein Profilbild. Darum solltest Du bei der Nutzung bewusst mit Deiner Privatsphäre umgehen. Bevor Du in Deinem Verein eine solche Chatgruppe einrichtest (beispielsweise für den Vorstand oder eine Mannschaft), ist es ratsam, mit allen geplanten Gruppenmitgliedern darüber zu sprechen.

DiNa-Tipp

DiNa-Tipp 9: Achte beim Instant Messaging auf Datensparsamkeit und Privatsphäre!

Deine Privatsphäre und Sicherheit kannst Du bei der Nutzung von Messenger-Diensten durch die folgenden Maßnahmen schützen:

- Verkürze oder anonymisiere Deinen **Nutzernamen**. In den meisten Fällen lassen sich die Profilangaben über die Messenger-Einstellungen nachträglich noch beliebig ändern.

- Gib bei Deinem **Profilfoto** möglichst wenig von Dir zu erkennen.

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

- Nimm nur Personen in Deine **Kontakte** auf, die Dir aus anderen Kontexten bekannt sind.

- Lehne Nachrichten sowie Anfragen für Dateiversand, Webcam- („Cam“) und Telefonfunktionen („Voice“) von **Unbekannten** generell ab. Auch diese Funktion kannst Du in den Privatsphäre-Einstellungen vornehmen.

- Versende keine sehr **privaten Bilder** oder wichtige Daten wie Passwörter, Bankdaten oder Kreditkartennummern.

Ausführlichere Informationen zu datensparsamen Messenger-Diensten findest Du bei der Verbraucherzentrale in dem Artikel „WhatsApp-Alternativen: die Datenschutzregeln im Überblick“. Gibt dazu auf der Website oben rechts in das Suchfeld den Begriff „WhatsApp-Alternativen“ ein. ▸ www.verbraucherzentrale.de

Recherchiere und vergleiche die Privatsphäre-Optionen und die Zugriffsrechte zweier Messenger-Dienste Deiner Wahl. Welchen Dienst würdest Du aus welchen Gründen vorziehen?

DiNa-Tipp

DiNa-Tipp 10: Achte bei der Videotelefonie auf die Sicherheitseinstellungen Deines Dienstes und auf Deine Privatsphäre!

Videotelefonie ist 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. Prüfe daher zunächst, ob Virenschutz, Firewall, Browser und Router aktuell sind. Nimm dann die Privatsphäre-Einstellungen in den Programmen selbst manuell vor. Hier kannst Du unter anderem auswählen, wer über das Programm Kontakt zu Dir aufnehmen darf.

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

- **Teile keine privaten Bilder** oder Informationen mit unbekannten Personen.

- **Achte darauf, was im Bild ist.** Große Teile Deiner Umgebung wie zum Beispiel Dein Büro, Deine Wohnung oder Dein Urlaubsort können Informationen für eine rechtswidrige Nutzung liefern.

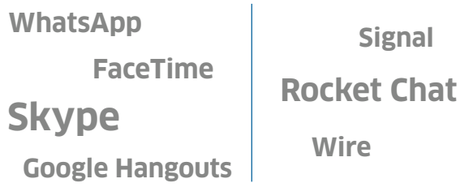
- **Logge Dich immer aus.** Kriminelle könnten über ein laufendes Programm auch auf andere Programme zugreifen, die parallel zum Videochat geöffnet sind, sogar auf Deine Kamera. Wenn Du Deine Kamera nicht nutzt, klebe diese mit einem Stück Klebezettel ab, damit sie nicht per Fernzugriff genutzt werden kann.

- Sei Dir bewusst, dass Videotelefonie-Teilnehmer*innen mit ihrem Programm **Mitschnitte der Gespräche** erstellen können. Solche gespeicherten Videos können zu Mobbing-Zwecken missbraucht werden.

Weitere Informationen zum Thema Cybermobbing findest Du im DiNa-Handbuch „Soziale Netzwerke: Kennenlernen, nutzen und souverän kommunizieren“.

Funktionen von Videotelefonie-Diensten

Der bekannteste Messenger-Dienst für Videotelefonie ist Skype. Daneben sind FaceTime, Google Hangouts sowie WhatsApp häufig genutzte Programme für Videotelefonie. Am besten orientierst Du Dich bei der Auswahl daran, welchen Dienst Deine Vereinskolleg*innen und Freund*innen nutzen.



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

Denn qualitativ und aus technischer Sicht gibt es bei den Angeboten keine großen Unterschiede, Voraussetzung ist allerdings ein ausreichend schneller Internetzugang. Das kannst Du beispielsweise unter speedtest.t-online.de testen. 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, kannst Du die Bildübertragung unterbrechen).

Auch bei der Anmeldung für Videotelefonie-Programme solltest Du auf Datensparsamkeit achten und nur die persönlichen Daten eingeben, die für die Nutzung des Programms wirklich benötigt werden.

Recherchiere die AGB eines Videotelefonie-Programms. Welche Probleme könnten sich durch die Videoübertragung ergeben? Welche Möglichkeiten haben Nutzer*innen, ihre Privatsphäre bei der Videotelefonie zu schützen?

Platz für Deine Notizen

Dein Verein tauscht sich aus

Checkliste

10 DiNa-Tipps: Online kommunizieren – aber sicher!

1. Schütze Dein E-Mail-Programm mit einem starken Passwort!
2. Nutze bei größeren Rundmails die E-Mail-Versandoption BCC!
3. Gehe sparsam mit der Angabe Deiner und anderer E-Mail-Adressen um!
4. Kommuniziere möglichst verschlüsselt!
5. Lösche E-Mails ungeöffnet, wenn sie Dir unseriös erscheinen und Dir die Absender*innen unbekannt sind!
6. Prüfe Deinen Rechner regelmäßig auf Schadprogramme!
7. Richte einen Spam-Filter ein!
8. Prüfe Zugriffe und Funktionen Deiner Messenger-Dienste!
9. Achte beim Instant Messaging auf Datensparsamkeit und Privatsphäre!
10. Achte bei der Videotelefonie auf die Sicherheitseinstellungen Deines Dienstes und auf Deine Privatsphäre!

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.
▸ https://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