Basisschutz für sichere E-Mail-Nutzung

E-Mails sind aus unserem Alltag kaum wegzudenken – wir nutzen sie zum Kommunizieren, für Verträge und fürs Onlineshopping oder zur Anmeldung bei unterschiedlichen Onlinediensten. Im Postfach fällt zwischen Newslettern, Paketbenachrichtigungen und Rechnungen eine Nachricht ins Auge: „Dringende Sicherheitswarnung – klicken Sie hier!“ Was tun? Ist die E-Mail echt? Oder steckt ein Betrugsversuch dahinter?

E-Mails verbinden Menschen, erleichtern den Alltag und ermöglichen einen schnellen Austausch – im Beruf und im Privatleben. Doch wo Vertrauen gefragt ist, versuchen Cyberkriminelle, es auszunutzen. Täuschend echte Nachrichten, gefälschte Absender und versteckte Schadsoftware gehören ebenso zum digitalen Alltag.

E-Mail-Sicherheit bedeutet, das eigene Postfach gut zu schützen, Methoden von Cyberkriminellen zu kennen und wachsam zu sein.

Deine E-Mails,
dein digitales Zuhause.

Tipps für mehr E-Mail-Sicherheit

Phishing und Identitätsdiebstahl verhindern

Bundesamt
für Sicherheit in der
Informationstechnik

Deine E-Mails,
dein digitales Zuhause.

8 Tipps für mehr E-Mail-Sicherheit

E-Mail-Kommunikation ist ein fester Bestandteil des digitalen Alltags – im Beruf und im Privatleben. Gleichzeitig ist das E-Mail-Postfach ein Einfallstor für Cyberangriffe. Ein bewusster und sicherer Umgang mit E-Mails ist daher unerlässlich. Dazu zählen grundlegende Schutzmaßnahmen wie starke Passwörter, die Nutzung einer Zwei-Faktor-Authentisierung oder die Verschlüsselung von E-Mails.
Außerdem spielen das Erkennen verdächtiger Nachrichten oder die Prüfung von Absenderadressen und Links eine wichtige Rolle.

1. Nutzen Sie ein einzigartiges starkes Passwort oder Passkeys.
2. Aktivieren Sie die Zwei-Faktor-Authentisierung.
3. Verschlüsseln Sie vertrauliche E-Mails.
4. Deaktivieren Sie die Anzeige von E-Mails im HTML-Format.
5. Nutzen Sie verschiedene E-Mail-Alias-Adressen.
6. Führen Sie regelmäßig Updates durch.
7. Aktivieren Sie Spam- und Phishing-Filter.
8. Achtung, Phishing: Bleiben Sie wachsam.

Schon gewusst?

IT-Sicherheitskennzeichen für E-Mail-Dienste

Mit dem IT-Sicherheitskennzeichen des BSI für E-Mail-Dienste sichern diese zu, dass ihre Produkte den Sicherheitsanforderungen des BSI entsprechen.

Nutzen Sie das IT-Sicherheitskennzeichen (IT-SiK) als Kriterium, wenn Sie ein neues E-Mail-Konto anlegen oder den Anbieter (Provider) wechseln bzw. Ihren Anbieter überprüfen möchten. Die Herstellererklärung für die Produktkategorie E-Mail-Dienste finden Sie auf der Website des BSI. Mit seiner Herstellererklärung hat der Diensteanbieter dem BSI gegenüber zugesichert, dass der Dienst die Technische Richtlinie für den sicheren E-Mail-Transport erfüllt, und er das BSI über bekannte Sicherheitslücken informiert und diese behebt.

Weiterführende Informationen

Weitere Informationen

Nutzen Sie die E-Mail wirklich sicher?

Spam, Phishing & Co.

E-Mail-Mythen im Faktencheck

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 87, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer:
BSI-IFB 25/154

1. Nutzen Sie ein einzigartiges starkes Passwort oder – wo möglich – Passkeys

Wählen Sie ein starkes Passwort und vergeben Sie für jeden Onlinedienst ein einzigartiges Passwort. Ein Passwort-Manager kann helfen, starke Passwörter zu erstellen und zu speichern. Als Alternative bieten immer mehr Anbieter inzwischen auch das Anmelden ohne Passwort mit Passkey an.

Ihr E-Mail-Konto ist besonders schützenswert! Wer möchte schon, dass Fremde unter dem eigenen Namen E-Mails verschicken, teure Waren im Internet kaufen oder die Passwörter anderer Dienste zurücksetzen? Um das zu verhindern, sollte ein Passwort schwer zu erraten und für jeden Dienst individuell sein. Ein kurzes und komplexes Passwort sollte mindestens acht Zeichen lang sein und aus vier verschiedenen Zeichenarten (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) bestehen. Sie können aber auch ein langes und weniger komplexes Passwort mit mindestens 25 Zeichen setzen. Passkeys hingegen beruhen auf einem kryptografischen Verfahren, das ohne Passworteingabe auskommt. Hier wird in der Regel als zweiter Faktor ein biometrisches Merkmal benutzt.

2. Aktivieren Sie die Zwei-Faktor-Authentisierung

Ergänzen Sie Ihr Passwort um eine zweite Sicherheitsstufe, z. B. einen Einmal-Code per App oder eine Bestätigung mit Fingerabdruck. Dadurch ist Ihr Konto auch dann geschützt, wenn Ihr Passwort durch ein Datenleak oder einen Hack in falsche Hände geraten ist.

Mittlerweile bieten viele E-Mail-Anbieter und Onlinedienste eine solche Zwei-Faktor-Authentisierung an. Es gibt sie in zahlreichen Varianten – vom individuellen Code per App bis hin zum hardware-gestützten TAN-Generator. Gelangt Ihr Passwort in die falschen Hände, ist Ihr E-Mail-Konto dennoch gut gesichert, da es durch die weitere Barriere eines zweiten Faktors vor fremdem Zugriff geschützt wird.

3. Verschlüsseln Sie vertrauliche E-Mails

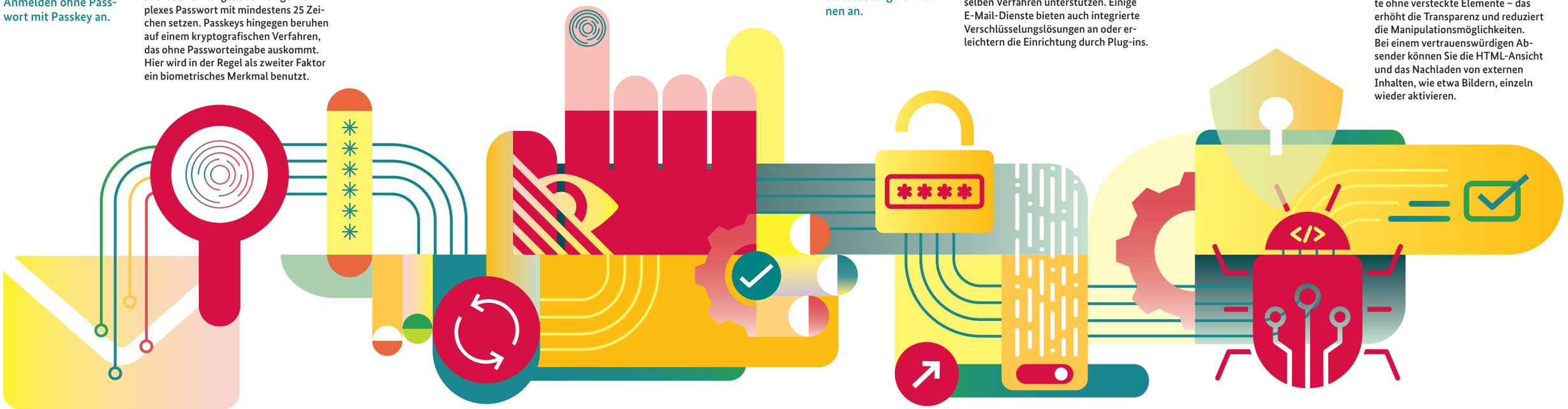
Ohne Verschlüsselung besteht das Risiko, dass Dritte Inhalte mitlesen, verändern oder missbrauchen. Nutzen Sie deshalb die Verschlüsselungsstandards S/MIME oder OpenPGP, um den Inhalt sensibler E-Mails zu schützen. Viele E-Mail-Anbieter bieten integrierte Verschlüsselungsfunktionen an.

E-Mails sind vergleichbar mit Postkarten: Ohne Verschlüsselung kann theoretisch jeder Ihre E-Mails lesen, der Zugriff auf den Übertragungsweg hat. Persönliche Daten, Vertragsunterlagen, sensible Inhalte oder vertrauliche Anhänge sollten daher verschlüsselt werden. Bei der Ende-zu-Ende-Verschlüsselung mit S/MIME oder PGP bzw. OpenPGP werden die Inhalte bereits beim Versenden verschlüsselt und erst wieder beim Empfänger entschlüsselt, sodass der gesamte Übertragungsweg geschützt ist. Wichtig ist, dass beide Seiten die Verschlüsselung mit demselben Verfahren unterstützen. Einige E-Mail-Dienste bieten auch integrierte Verschlüsselungslösungen an oder erleichtern die Einrichtung durch Plug-ins.

4. Deaktivieren Sie die Anzeige im HTML-Format

Im sogenannten Quellcode einer HTML-formatierten E-Mail lauert mitunter schädlicher Code, der bereits beim Öffnen der E-Mail auf dem Gerät des Empfängers oder der Empfängerin ausgeführt wird. So kann z. B. ein Schadprogramm installiert werden.

Die Anzeige von E-Mails im HTML-Format ermöglicht zwar eine ansprechende Gestaltung, birgt jedoch Sicherheitsrisiken. Cyberkriminelle nutzen HTML-E-Mails, um Schadprogramme einzuschleusen, Tracking-Pixel einzubetten oder gefälschte Links zu tarnen. So kann schon das Öffnen der E-Mail Informationen über den Standort oder die Aktivitäten des Empfängers oder der Empfängerin preisgeben. Deaktivieren Sie daher die HTML-Anzeige und nutzen Sie stattdessen die Nur-Text-Ansicht. Diese zeigt die reinen Inhalte ohne versteckte Elemente – das erhöht die Transparenz und reduziert die Manipulationsmöglichkeiten. Bei einem vertrauenswürdigen Absender können Sie die HTML-Ansicht und das Nachladen von externen Inhalten, wie etwa Bildern, einzeln wieder aktivieren.



5. Nutzen Sie verschiedene E-Mail-Alias-Adressen

Verwenden Sie separate E-Mail-Alias-Adressen für private Kommunikation und Onlineregistrierungen, wie Newsletter, Foren und Onlineshops. Die Nutzung unterschiedlicher Adressen, sogenannter Aliasse, in einem E-Mail-Konto hilft, den digitalen Alltag übersichtlicher und sicherer zu gestalten.

Neben Ihrer eigentlichen E-Mail-Adresse vorname.nachname@beispiel.de für wichtige Kommunikation – etwa mit Behörden oder Banken – legen Sie beispielsweise den Alias nachname-shopping@beispiel.de für Onlinebestellungen und einen weiteren Alias für Newsletter an. Durch diese Trennung behalten Sie etwa mithilfe unterschiedlicher Ordner für die einzelnen E-Mail-Adressen besser den Überblick im Postfach. Darüber hinaus können Sie Ihre persönlichen Daten besser schützen: Wird eine Alias-Adresse durch ein Leak oder einen Hack beispielsweise zum Ziel von Spam, können Sie diese löschen oder ändern, ohne dass das komplette Postfach betroffen ist. Viele E-Mail-Anbieter erlauben das Erstellen zusätzlicher E-Mail-Alias-Adressen zu einem E-Mail-Konto.

6. Führen Sie regelmäßig Updates durch

Halten Sie Ihr Betriebssystem, Ihr E-Mail-Programm und Ihr Virenschutzprogramm immer auf dem neuesten Stand, um bekannte Sicherheitslücken zu schließen. Aktivieren Sie nach Möglichkeit automatische Updates.

Betriebssysteme, Virenschutzprogramme und E-Mail-Dienste werden ständig weiterentwickelt. Dabei werden nicht nur neue Funktionen bereitgestellt, sondern auch Sicherheitslücken geschlossen. Cyberkriminelle nutzen Sicherheitslücken aus, um etwa Schadprogramme einzuschleusen oder persönliche Daten abzugreifen. Updates sollten deshalb immer zeitnah, am besten automatisch, installiert werden. E-Mail-Programme bzw. die oft zusätzlich von Webmail-Diensten angebotenen Apps sollten regelmäßig aktualisiert werden, um Cyberkriminellen Datendiebstahl und Infektionen mit Schadprogrammen zu erschweren.

7. Aktivieren Sie Spam- und Phishing-Filter

Nutzen Sie die Sicherheitsfunktionen Ihres E-Mail-Anbieters, um verdächtige E-Mails automatisch herauszufiltern. Viele Dienste bieten Optionen zur Erkennung und Blockierung von Phishing-Mails an.

Spam- und Phishing-Filter sind wichtige Schutzmaßnahmen für jedes Postfach. Sie erkennen und blockieren unerwünschte Spam- oder gefährliche Phishing-Nachrichten, bevor sie überhaupt im Posteingang landen. So werden Sie automatisch vor betrügerischen Inhalten, Schadsoftware oder unseriösen Angeboten geschützt. Moderne Filter können Absender, Inhalte, Anhänge und Links automatisiert analysieren und verdächtige E-Mails erkennen. Somit wird das Risiko reduziert, dass Sie versehentlich oder unter Zeitdruck auf gefälschte E-Mails hereinfallen.

8. Achtung, Phishing: Bleiben Sie wachsam

Nervige E-Mails verstopfen nicht nur E-Mail-Postfächer, sondern können auch das Empfängersystem mit einem Schadprogramm, etwa zum Ausspionieren persönlicher Daten, infizieren. Phishing-Mails werden zunehmend besser und die Betrugsmaschen immer perfider – meist mit dem Ziel, den Nutzer oder die Nutzerin zur Preisgabe persönlicher Daten auf gefälschten Webseiten zu bewegen.

Öffnen Sie keine Anhänge und klicken Sie nicht auf Links in unerwarteten oder verdächtigen E-Mails, auch wenn sie von scheinbar bekannten Absendern stammen. Prüfen Sie die Absenderadresse und die URL durch ein Mouseover, bevor Sie darauf klicken. Seien Sie misstrauisch bei unerwarteten Anhängen oder Dateiendungen wie .exe, .zip oder anderen kryptischen Formaten. Auch ungewöhnliche Sprachmuster, holprige Formulierungen, Zeitdruck, Drohungen oder angeblich dringende Aktionen sollten stutzig machen. Reagieren Sie nicht voreilig und geben Sie niemals persönliche Daten preis. Unternehmen und Behörden fragen nie per E-Mail nach Passwörtern, Bankdaten oder anderen vertraulichen Informationen.