Halten Sie Ihre Apps und Software auf dem neuesten Stand.

Patches sind wichtig, weil sie bekannte Produktschwachstellen beheben, die Angreifer ausnutzen können, um Ihre Geräte zu kompromittieren.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

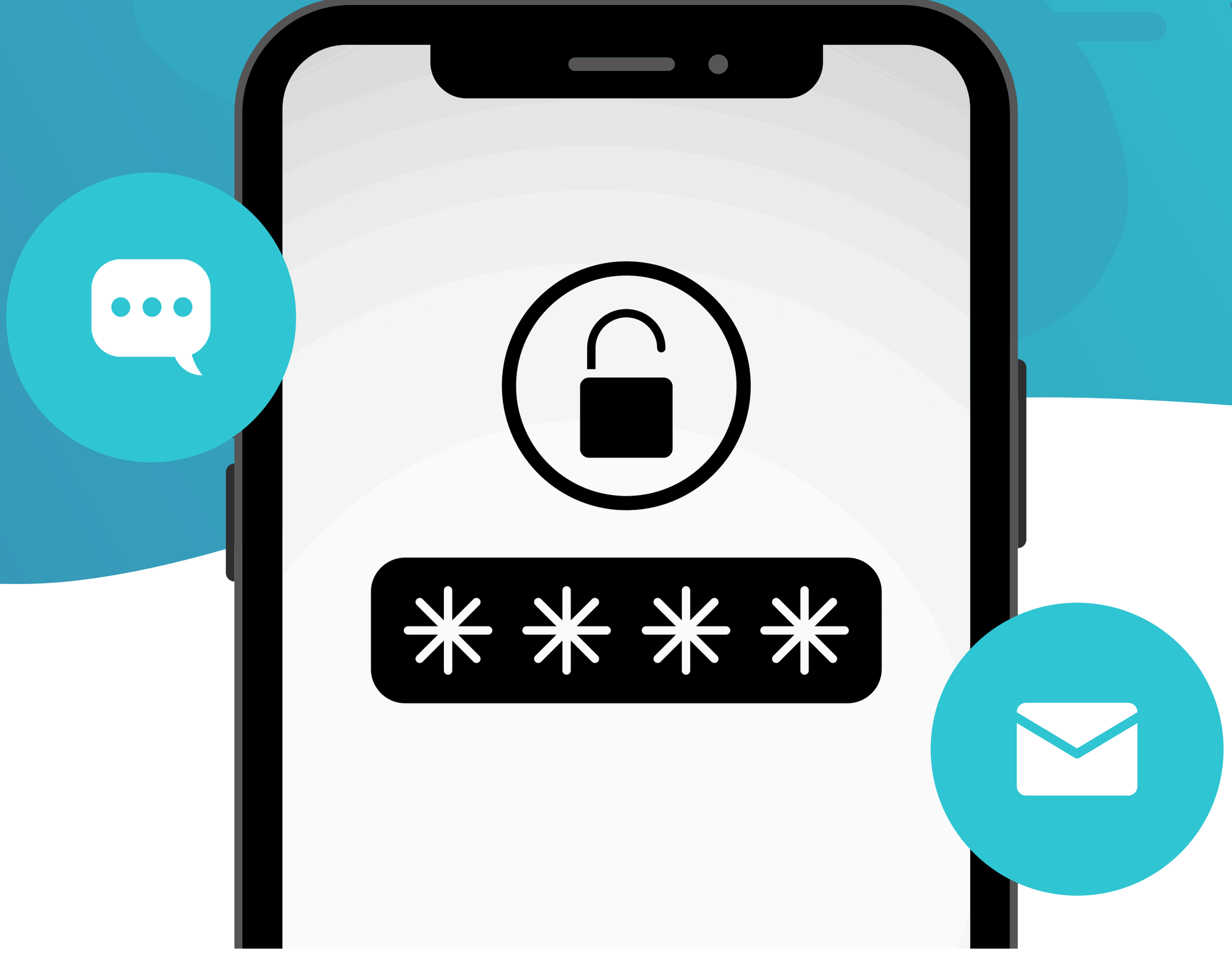
Multi-Faktor-Authentifizierung (MFA) aktivieren

Die Multi-Faktor-Authentifizierung (MFA) schützt Ihre Konten und Geräte, indem sie Sie auffordert, Ihre Identität mehrmals nachzuweisen.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA).

Die Zwei-Faktor-Authentifizierung (2FA) schützt Ihre Konten und Geräte, indem sie Sie auffordert, Ihre Identität mehrmals nachzuweisen.



Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Stellen Sie sicher, dass Ihr Heimnetzwerk sicher ist.

Das Ändern des Standardpassworts Ihres Routers und die Aktualisierung Ihrer Firmware tragen dazu bei, das Risiko eines Hackerangriffs zu verringern.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Warum sollte man ein VPN zur Verbesserung der Sicherheit nutzen?

Eine Verbindung zu einem virtuellen privaten Netzwerk (VPN) maskiert Ihren Online-Datenverkehr und schützt ihn vor externem Zugriff.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Vergessen Sie nicht die physische Sicherheit.

Vergessen Sie nicht, Ihren Computer zu sperren, wenn Sie das Büro verlassen, und bewahren Sie alle Papierdokumente mit vertraulichen Informationen unter Verschluss auf.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Teilen Sie vertrauliche Informationen in sozialen Medien?

Cyberkriminelle können die Informationen, die Sie in sozialen Medien veröffentlichen, nutzen, um personenbezogene Daten (PII) über Sie zu erhalten, die gegen Sie verwendet werden können.

Bleiben Sie wachsam.
Informieren Sie sich über Cyberrisiken.

Beachten Sie stets die Unternehmensrichtlinien und -verfahren.

Sicherheitsrichtlinien und -verfahren liefern wichtige Leitlinien, die uns helfen, unser Unternehmen, unsere Kollegen und unsere Kunden vor Cyberangriffen und Datenverlust zu schützen.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Vorsicht vor Social Engineering

Social Engineering ist eine Angriffsmethode, die auf menschlicher Interaktion beruht und häufig darin besteht, Menschen zur Verletzung von Sicherheitsvorkehrungen zu manipulieren, um Zugang zu Systemen, Netzwerken oder physischen Standorten zu erlangen.

Bleiben Sie wachsam.
Informieren Sie sich über Cyberrisiken.

5 verräterische Anzeichen eines Social-Engineering-Angriffs

Die Nachricht kommt unerwartet an.

Dies ist ein Hauptmerkmal von Social Engineering, obwohl Angreifer auch kompromittierte E-Mail-Konten nutzen können, um Konversationen zu kapern.

Die geforderte Aktion erscheint ungewöhnlich.

Seien Sie vorsichtig, wenn Sie aufgefordert werden, etwas zu tun, was Sie normalerweise nicht tun würden (z. B. Geld senden, etwas installieren, Kundendaten weitergeben usw.).

Die geforderte Maßnahme erscheint riskant.

Könnte diese Maßnahme dem Empfänger oder dem Unternehmen schaden? Wenn ja, überlegen Sie es sich gut.

Ein ungewöhnlicher Anhang oder eine URL

Viele Social-Engineering-Betrügereien beinhalten einen betrügerischen Link, auf den der Benutzer klicken soll, oder ein Dokument/Programm zum Herunterladen.

Es herrscht ein Gefühl der Dringlichkeit.

Viele Betrugsmaschen basieren auf einem starken Gefühl der Dringlichkeit, und der Betrüger versucht, eine Bedrohung durch Schaden zu vermitteln.

Bleiben Sie wachsam.
Informieren Sie sich über Cyberrisiken.

Fallen Sie nicht auf Phishing-Betrügereien herein!

Phishing-E-Mails sehen aus wie legitime Anfragen von bekannten Institutionen und fordern Sie oft auf, auf Links zu klicken, Anhänge herunterzuladen oder sensible Informationen preiszugeben.

Überlegen Sie es sich gut, bevor Sie klicken.

Bleiben Sie wachsam.
Informieren Sie sich über Cyberrisiken.

Tipps zur Sensibilisierung für Phishing

Verdächtige Links in E-Mails

Seien Sie vorsichtig, wenn die Webadresse, die beim Überfahren des Links mit der Maus erscheint, nicht mit dem Absender übereinzustimmen scheint oder wenn die E-Mail Sie auf eine Seite weiterleitet, auf der Sie sich anmelden müssen.

Schlechte Rechtschreibung und Grammatik

Phishing-E-Mails und -SMS können mitunter voller Rechtschreib- und Grammatikfehler sein, achten Sie daher auf diese Anzeichen.

Anfrage nach sensiblen Informationen

Wenn Sie aufgefordert werden, vertrauliche Informationen preiszugeben, die Sie normalerweise nicht per E-Mail weitergeben würden, rufen Sie eine Ihnen bekannte Telefonnummer an, um die Anfrage zu überprüfen.

Notfall oder zugrunde liegende Bedrohungen

Angreifer nutzen oft ein Gefühl der Dringlichkeit aus, um Sie unter Druck zu setzen und Sie zu schnellem Handeln zu bewegen, ohne Ihnen Zeit zum Innehalten und Nachdenken zu lassen.

Verdächtige Domänen

Viele bösartige E-Mails verwenden eine Domain, die legitim aussieht, aber kleine Unterschiede aufweist.

Bleiben Sie wachsam.
Informieren Sie sich über Cyberrisiken.

Verwenden Sie stets starke, einzigartige und vertrauliche Passwörter.

Ihre Passwörter sollten einzigartig, privat und für Sie leicht zu merken, aber für Hacker nicht leicht zu erraten sein.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.

Tipps zur Passwortsicherheit

Verwenden Sie Ihre Passwörter nicht wieder.

Wenn ein Datenleck eines Ihrer Konten kompromittiert, könnte der Angreifer mithilfe Ihrer wiederverwendeten Passwörter auf andere Konten zugreifen.

Lassen Sie Ihre Passwörter nicht offen herumliegen.

Bewahren Sie Ihre Passwörter nicht an einem unsicheren Ort auf, wie z. B. auf einem Haftzettel, in einem Terminkalender oder in einer unverschlüsselten Textdatei.

Geben Sie Ihre Passwörter nicht weiter.

Geben Sie Ihre Passwörter oder Kontodaten niemals an irgendjemanden weiter, nicht einmal an Ihre Kollegen.

Erstellen Sie lange und einfache Passwörter.

Verwenden Sie eine Reihe scheinbar unzusammenhängender Wörter, um lange, einfache statt kurzer, komplexer Passwörter zu erstellen.

Multifaktor-Authentifizierungsmethoden verwenden

Nutzen Sie die sicherste verfügbare Methode der Multi-Faktor-Authentifizierung, z. B. eine Authentifizierungs-App.

Bleiben Sie wachsam. Informieren Sie sich über Cyberrisiken.