RESOURCE CENTER

Monat des Bewusstseins für Cybersicherheit

Get the full interactive view at
https://bitwarden.com/de-de/resources/cybersecurity-awareness-month/

bitwarden

Einfache Cybersicherheit: 4 Schritte zur Online-Sicherheit

> „Der Cybersecurity Awareness Month, der jeden Oktober stattfindet, ist eine Zusammenarbeit zwischen Regierung und Privatwirtschaft, um das Bewusstsein für digitale Sicherheit zu schärfen und es jedem zu ermöglichen, seine persönlichen Daten vor digitalen Formen der Kriminalität zu schützen."

- Nationale Cybersicherheitsallianz

Inhaltsverzeichnis

Starke und einzigartige Passwörter

Multi-Faktor-Authentifizierung verwenden

Halten Sie Ihre Software auf dem neuesten Stand

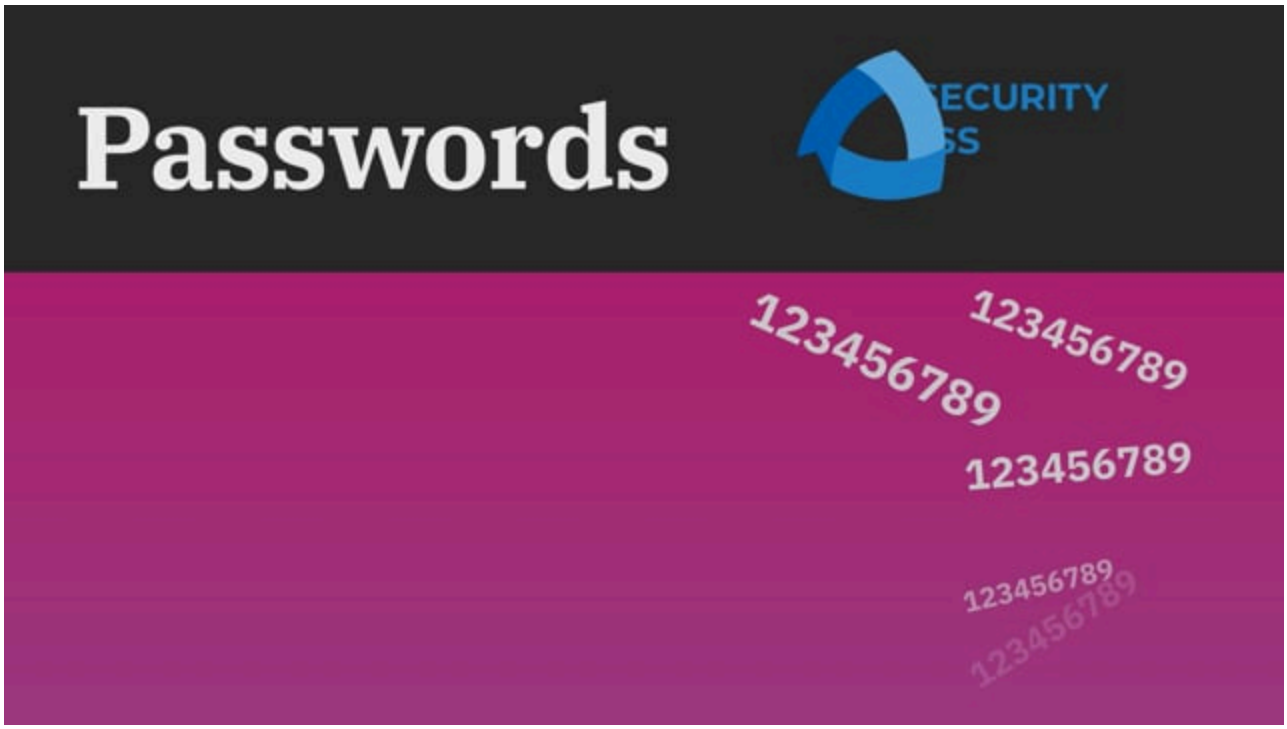
So erkennen Sie einen Phishing-Betrug

Zusätzliche Ressourcen

Schritt 1. Starke und einzigartige Passwörter bilden die Grundlage für Cybersicherheit

Täglich meldet sich die durchschnittliche Person bei einer Variation von Instagram, TikTok, Bank-Apps, Geschäftskonten, persönlichen E-Mails, E-Commerce-Websites und Mitfahrgelegenheiten an. Man kann mit Fug und Recht sagen, dass wir in einer Online-Welt leben.

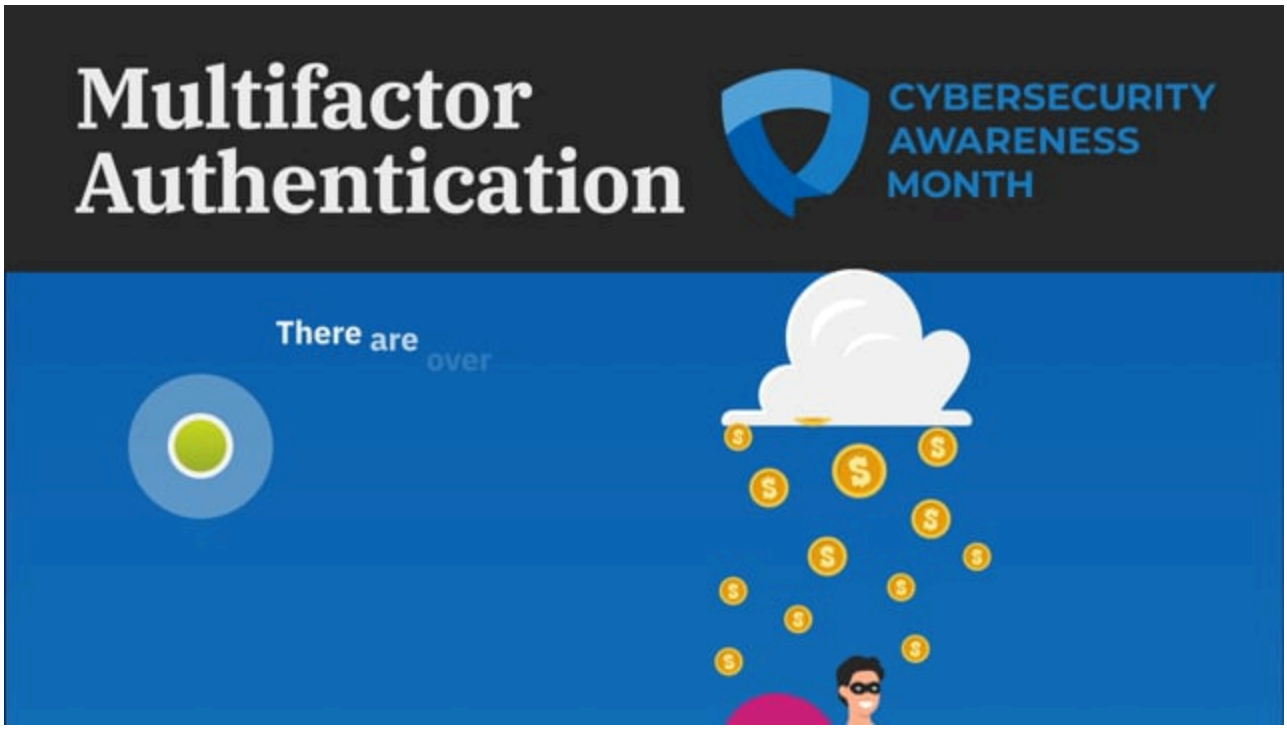
Wie können Benutzer, die so viele Informationen austauschen, sicher bleiben? Es ist eigentlich ganz einfach. Die Verwendung starker und eindeutiger Passwörter trägt zum Schutz Ihrer Daten bei. Du bist dir nicht sicher, ob deine Passwörter stark genug sind? Testen Sie ihre Stärke und erfahren Sie mehr über die Passwortverwaltung. Sie können jetzt auch mit einem voll ausgestatteten kostenlosen Konto für unbegrenzte Anmeldungen auf unbegrenzten Geräten beginnen.



https://player.vimeo.com/video/752654111

Schritt 2. Verwenden Sie die Multi-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA), die zweistufige Anmeldung oder die Multi-Faktor-Authentifizierung (MFA) bezieht sich auf die separaten Methoden zur Überprüfung der Identität, um auf ein Konto zuzugreifen. Dies kann die Anmeldung bei einem Konto mit einem Passwort und die anschließende erneute Bestätigung mit einem Authentifizierungscode umfassen. Eine detailliertere Erklärung finden Sie in diesem Beitrag für die Top 10 der brennenden Fragen zu 2FA und weitere Informationen zu verschiedenen Methoden für 2FA/MFA finden Sie in diesem zweistufigen Login-Hilfeartikel. Einfach ausgedrückt, bietet die zweistufige Anmeldung die zusätzliche Schutzebene, die jeder benötigt.



https://player.vimeo.com/video/752706739

Besuchen Sie den Umfrageraum: eine Sammlung von Umfragen und Berichten zu Passwortverwaltung und Sicherheit für Unternehmen und Einzelpersonen.

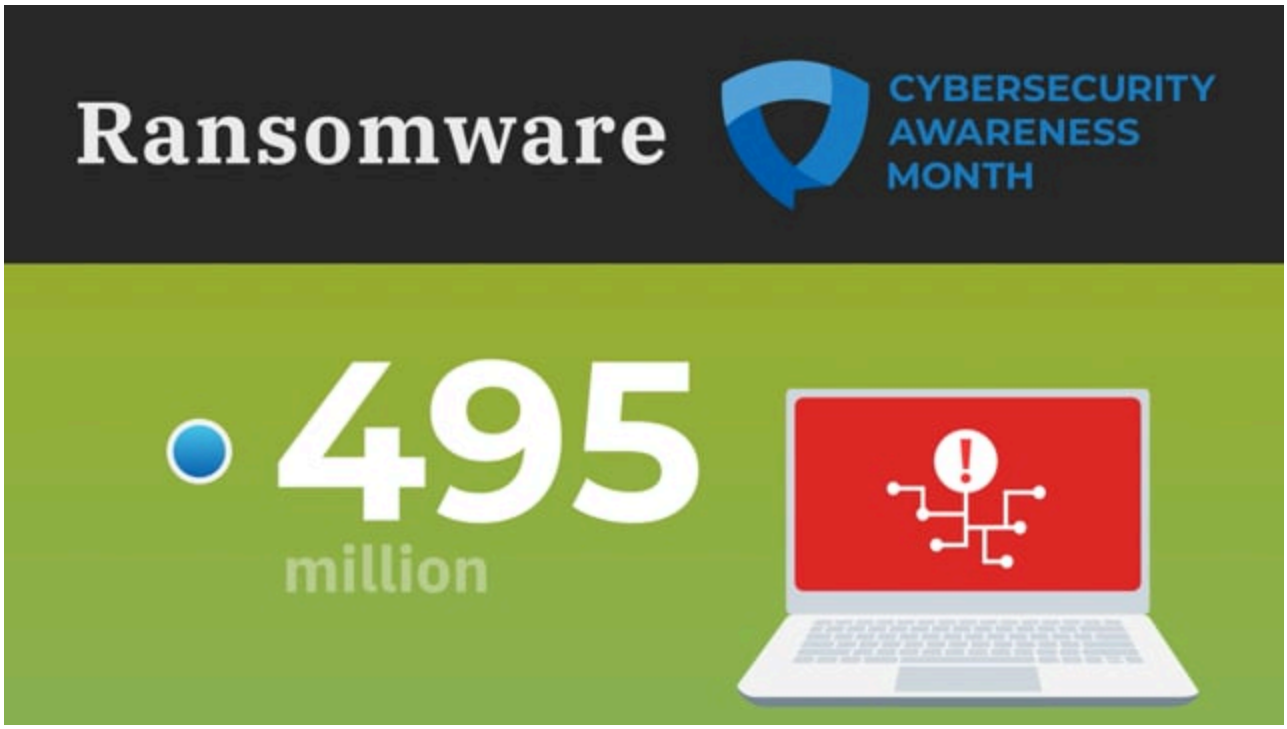
Did you know?

Passkey 2FA is included in every Bitwarden plan, including free! All users can secure their Bitwarden account with a hardware security key or other FIDO2 WebAuthn credential generator.

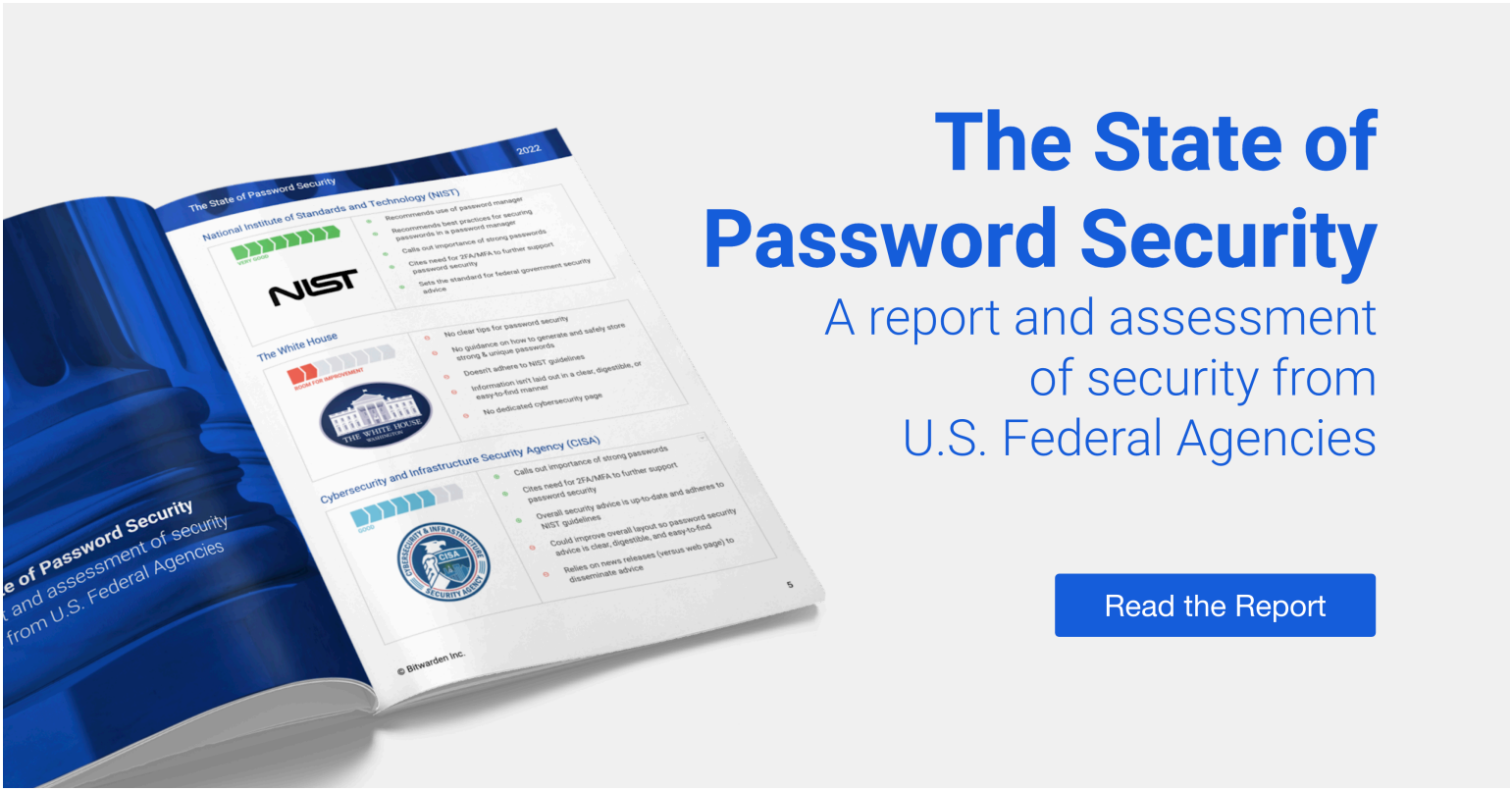
Schritt 3. Halten Sie Ihre Software auf dem neuesten Stand

Der Cybersecurity Awareness Month erinnert alle daran, über Software-Updates auf dem Laufenden zu bleiben. In der Regel beheben Updates Sicherheitslücken, entfernen Fehler und fügen Funktionen hinzu, die Informationen besser schützen können. Es ist zwar verlockend, auf die Updates zu verzichten, aber ein paar Minuten Updates könnten stundenlange Kopfschmerzen aufgrund einer gestohlenen Identität verhindern.

Software-Updates helfen auch, Ransomware-Angriffe zu verhindern. Typischerweise versuchen lösegeldorientierte Cyberkriminelle, Schwachstellen auszunutzen - einschließlich Schwachstellen wie veraltete Software.



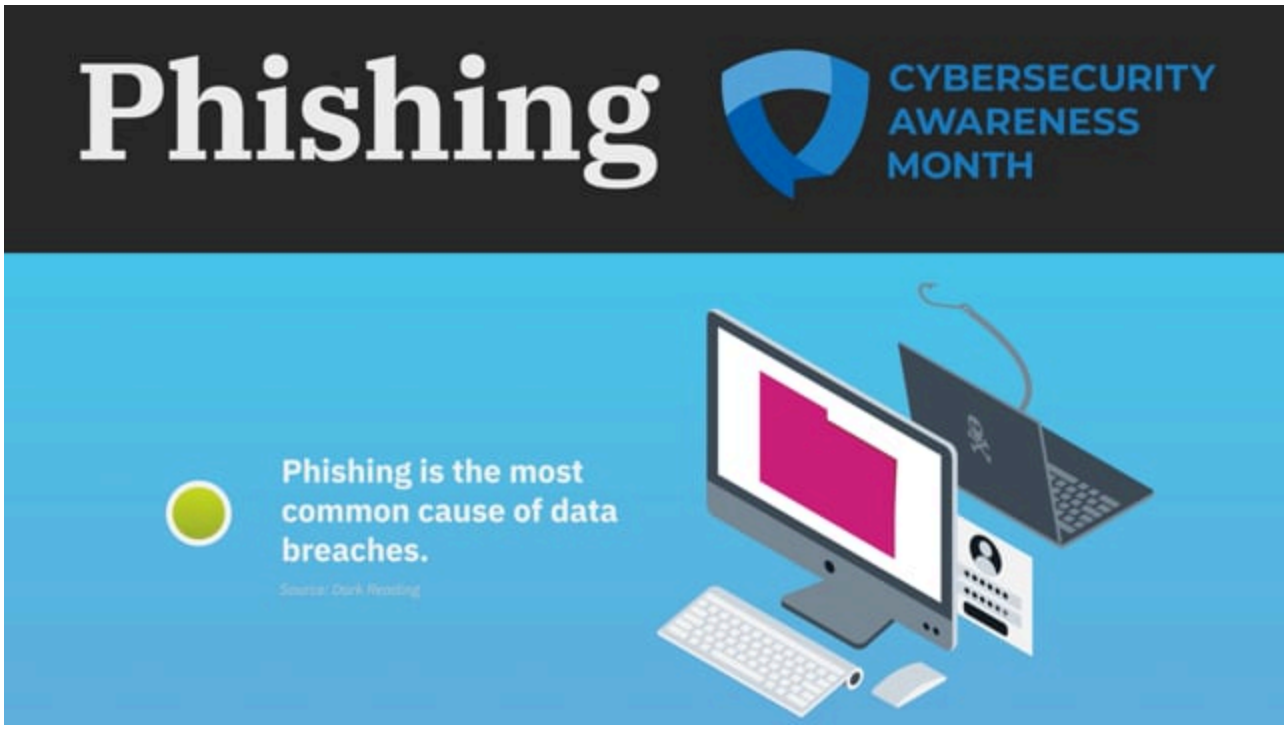
https://player.vimeo.com/video/752707997



Schritt 4. Wissen, wie man einen Phishing-Betrug erkennt

Erfahren Sie, wie Sie auf Phishing-Angriffe achten können, die sich auf den Versuch beziehen, Menschen dazu zu bringen, wertvolle Daten zu teilen oder mit Malware infizierte Websites zu besuchen. Benutzer sollten überprüfen, ob E-Mails vom richtigen Absender kommen, den Mauszeiger über Links bewegen, um zu bestätigen, dass sie zur richtigen Website gehen, und vermeiden, Anhänge von Personen zu öffnen, die sie nicht kennen. Seien Sie besonders vorsichtig bei mobilen Geräten, die nicht immer die Hover-Option haben, um genaue E-Mail-Adressen und Link-Ziele zu sehen.

Darüber hinaus können Tools wie Passwort-Manager helfen. Lesen Sie mehr darüber, wie Passwort-Manager helfen, Phishing zu verhindern.



https://player.vimeo.com/video/752708367

Zusätzliche Ressourcen

- 7 Schritte zum Erstellen eines sicheren und privaten Online-Profils
- Der Vermessungsraum
- Warum Unternehmen einen Passwort-Manager benötigen
- Was die passwortlose Einführung für Unternehmen bedeutet
- Qualifizierung für Cyber-Versicherung mit sicherer Passwortverwaltung
- Die Vorteile der Passwortverwaltung als Service
- Wertsteigerung für Bitwarden-Benutzer - Bitwarden sammelt 100 Millionen US-Dollar
- Erfahren Sie, was die Experten über Bitwarden sagen

Nehmen Sie an diesem Cybersecurity Awareness Month für mehrere Twitter Spaces mit dem Bitwarden-Team zu spannenden Cybersicherheitsthemen teil! Folgen Sie uns auf Twitter, damit Sie den Spaß nicht verpassen.

Anatomy of Cybersecurity: How to Stay Secure at Work & at Home

Download PDF

4 Steps to Simple Security

Download PDF