RECIPE
Recentering The Civic Internet
Through Partner Engagement

دليل استخدام أدوات الأمان الرقمي

الدليل العملي

OXFAM

Alkhatt

RECIPE
Recentering The Civic Internet Through Partner Engagement

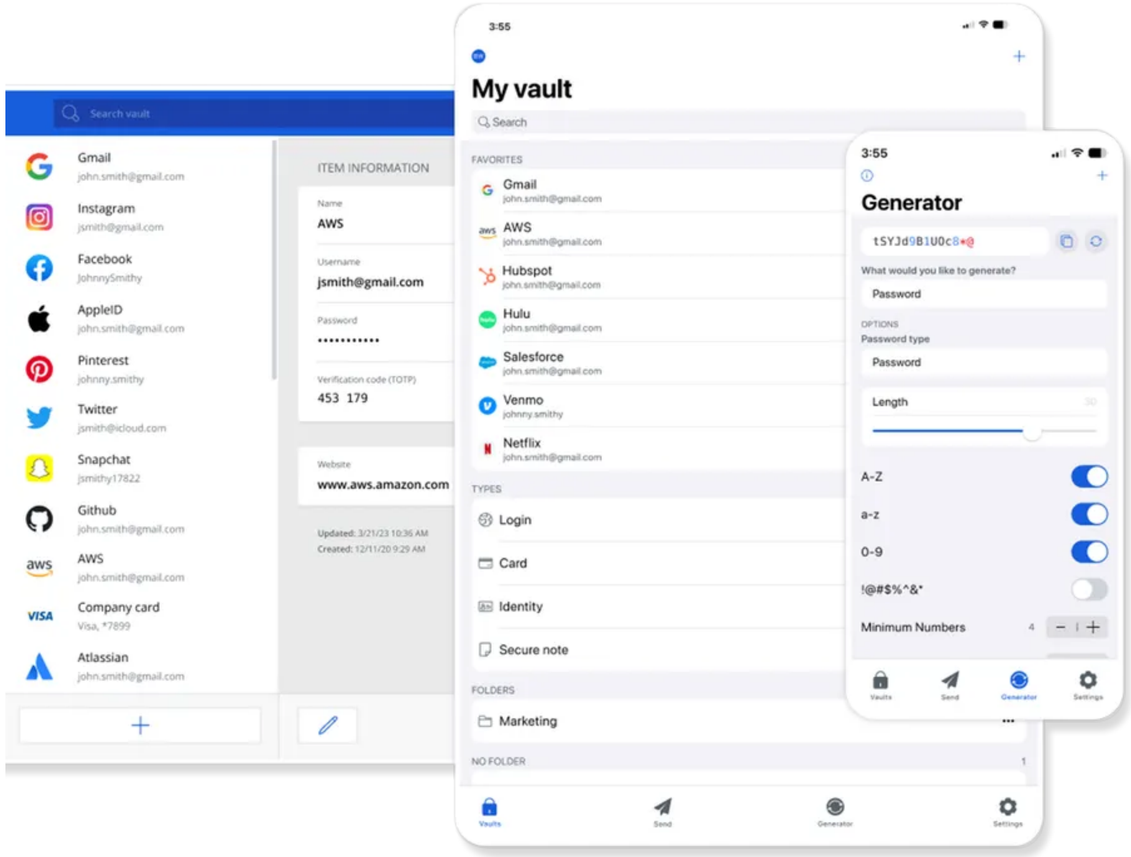
استخدم هذا الدليل لمساعدتك على بناء مخططك الشخصي للأمان الرقمي

RECIPE
Recentering The Civic Internet Through Partner Engagement

البيئة الرقمية الشخصية

لتجهيز الخطة الشخصية للأمان الرقمي، يجب الانطلاق بحصر البيئة الرقمية الشخصية من حسابات رقمية، أجهزة، وتطبيقات تستخدمها يوميًا.

هذا الحصر مهم لبناء خطة تأمين شاملة ومستدامة.



RECIPE
Recentering The Civic Internet Through Partner Engagement

من أجل حسابات آمنة

- الحرص على إنشاء حسابات رقمية فقط عند الحاجة
- التأكد من استخدام أساليب متعددة للاسترداد وللوصول للحسابات
- استخدام أساليب استرداد مؤمَّنة، كأرقام هاتف وعناوين بريد إلكتروني آمنة
- التأكد من حذف الحسابات الرقمية في حالة عدم الحاجة لها

RECIPE
Recentering The Civic Internet Through Partner Engagement

حماية الحسابات بكلمة مرور قوية وغير متكررة

كلمة المرور الصعب التنبؤ بها وغير المتكرر استخدامها على أكثر من موقع أو حساب هي خط الدفاع الأول لحضورك الرقمي وبنيتك الرقمية.

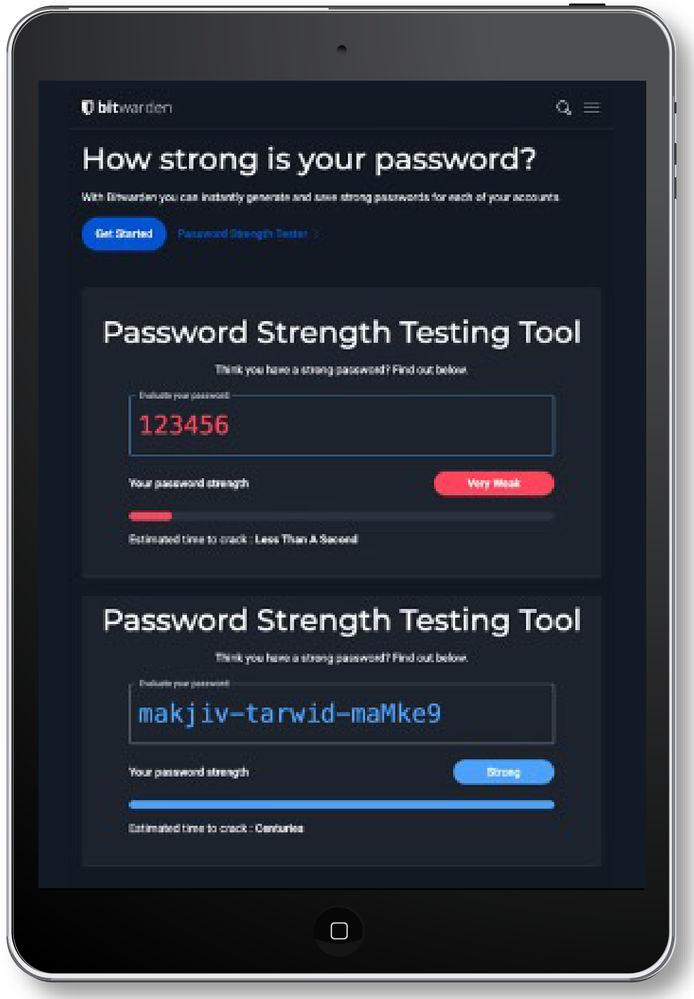
RECIPE
Recentering The Civic Internet
Through Partner Engagement

اختبر قوة كلمة مرورك

Bitwarden password strength

هي أداة آمنة تمكّنك من اختبار
كلمة المرور التي تستعملها
والتأكد من قوتها، كما تساعدك
على اختيار كلمات مرور قوية.

https://bitwarden.com/password-strength/



كيف يمكننا تذكر كلمات المرور المعقّدة؟

لا تحتفظ بكلمات المرور في مكان غير آمن أو يسهل الوصول إليه.

يُنصح باستخدام أدوات إدارة كلمات المرور Password Manager.

في المتصفح أو في الهاتف، يمكن استخدام تطبيقات حفظ كلمات المرور، واستعمالها كمكان واحد وآمن للتخزين.

RECIPE
Recentering The Civic Internet Through Partner Engagement

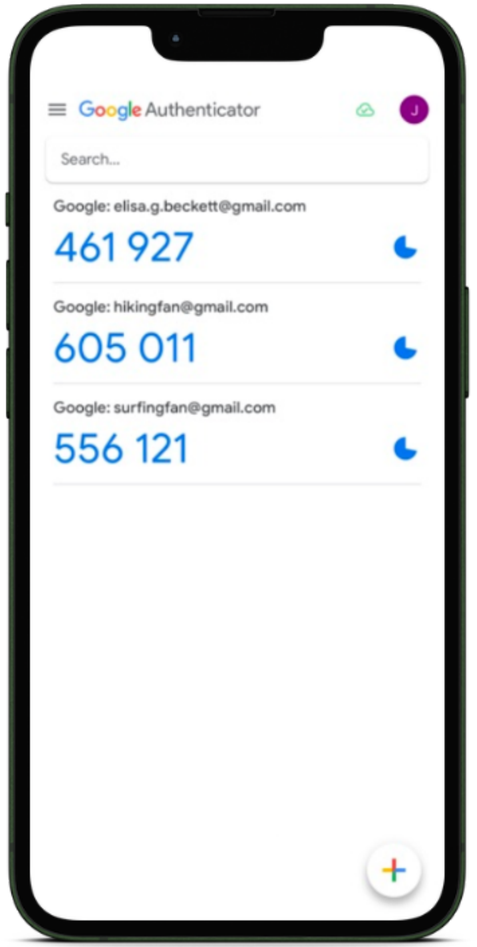
حماية إضافية للحسابات

MFA Authentication

طبقة إضافية من الحماية تمكّنك من تأمين الوصول إلى الحسابات الرقمية عبر رمز أمان متغيّر يُدار عبر تطبيق على الهاتف.

https://bitwarden.com/download/#bitwarden-authenticator-mobile

بدائل موثوقة: Authy, Google Authenticator



RECIPE
Recentering The Civic Internet Through Partner Engagement

من أجل أنظمة آمنة

- الحرص على استعمال برمجيات وأنظمة أصلية ومفعّلة
- التأكد من تحديث جميع الأنظمة والبرمجيات الأساسية بشكل دوري
- استخدام برمجيات آمنة وموثوقة، وتجنب تحميل التطبيقات من مواقع أو متاجر غير أصلية
- استخدام برمجيات أو أنظمة حرّة ومفتوحة المصدر كبدائل آمنة ومستدامة

RECIPE
Recentering The Civic Internet
Through Partner Engagement

تحديث الأنظمة والتطبيقات

الحرص على تفعيل التحديث الآلي أو التحديث الدوري للأنظمة والتطبيقات ذات الأهمية، مثل أنظمة التشغيل في الحواسيب والهواتف، وتطبيقات التصفح، ومضادات الفيروسات، وغيرها من التطبيقات التي تُستخدم يوميًا.

- تفعيل تطبيقات الحماية ومضادات البرمجيات الخبيثة مثل برامج مضادات الفيروسات أو تطبيقات مرافقة لأنظمة التشغيل مثل **Windows Defender**.

- التأكد من الاستخدام السليم لتطبيقات الحماية والتدقيق الدوري في سلامة الأنظمة والملفات من البرمجيات الخبيثة. كما يُنصح بالاستفادة من الخصائص المتقدمة التي توفرها برامج مضادات الفيروسات، مثل حماية الأجهزة في حالات السرقة وتتبعها.

RECIPE
Recentering The Civic Internet Through Partner Engagement

تأمين الشبكات والاتصال

- استخدام شبكات Wi-Fi آمنة ومشفرة، وتجنب الشبكات العامة المفتوحة قدر الإمكان
- استخدام VPN عند الاتصال بشبكات غير موثوقة أو أثناء السفر
- التأكد من تحديث إعدادات الراوتر وكلمات مرور الشبكة بشكل دوري

RECIPE
Recentering The Civic Internet Through Partner Engagement

من أجل بيانات آمنة

- أقل أساليب حماية البيانات تكلفة هو عدم تجميعها من الأساس أو التخلص بشكل دوري من البيانات غير الضرورية.

- خطة تأمين البيانات المستدامة تحتاج إلى تصنيف البيانات بناءً على الأهمية والحساسية، ليتم تجهيز خطة تأمين خاصة لكل صنف.

- الحرص على أن تشمل خطة تأمين البيانات سياسة تحديث دوري للبيانات المخزنة طويلة المدى والنسخ الاحتياطية.

- التأكد بشكل دوري من استدامة خطة التأمين لتتوافق مع التغييرات في أساليب أو بيئة العمل.

مقترح لتصنيفات البيانات

بيانات أساسية

مهمة وتُستخدم بشكل يومي، فقدان الوصول إليها قد يؤثر على سير العمل، لكن تسريبها لا يمثل خطرًا كبيرًا.

استخدام خدمات سحابية توفر التحديث اللحظي مع خاصية العمل المشترك.

بيانات استراتيجية

غير ذات أهمية مباشرة في العمل اليومي، مثل الأرشفة طويلة المدى للفيديوهات، قد لا يشكل تسريبها خطرًا كبيرًا، مع أهمية الحفاظ عليها.

استخدام نسخ احتياطية متعددة على أقراص خارجية أو خدمات سحابية، ووضع الأقراص في أماكن آمنة.

بيانات حساسة

موضوع التزامات قانونية وأخلاقية. لا تُستخدم بشكل يومي، ويسمح لعدد قليل فقط من الأشخاص بالوصول إليها، وتسريبها يشكّل خطرًا كبيرًا جدًا.

استخدام نسخ احتياطية مشفّرة على أقراص خارجية حصريًا، ووضع الأقراص في أماكن آمنة.

RECIPE
Recentering The Civic Internet Through Partner Engagement

من أجل أجهزة آمنة

- الحرص على إبقاء الأجهزة في أماكن آمنة وعدم التنقل بها إلا عند الحاجة
- قفل الأجهزة بكلمات مرور قوية وتفادي استخدام أساليب قفل ضعيفة
- تفادي تخزين بيانات حساسة على الأجهزة، خاصة الهواتف
- استخدام خاصيات التتبع وحذف البيانات عن بُعد في حالة السرقة أو الضياع

قفل هاتف آمن

من البديهي وجوب استخدام قفل لجميع الأجهزة، ويُستحسن في حالات الحاجة استخدام أقفال أكثر أمانًا للهواتف، مثل كلمات المرور بدل الرموز سهلة التنبؤ بها. كما يُنصح بتجنب الاعتماد على القفل بالبيانات البيومترية، مثل البصمة أو التعرف على الوجه.

RECIPE
Recentering The Civic Internet Through Partner Engagement

من أجل خصوصية أكثر

- التأكد من طلب حذف البيانات عند حذف الحسابات الرقمية
- التثقيف المستمر حول الأثر الرقمي الذي نتركه عند استخدام المواقع والتطبيقات
- التأكد من إعدادات الخصوصية في المنصات الرقمية ومختلف الخدمات الرقمية
- التأكد من أذونات الوصول التي نمنحها للتطبيقات والمواقع، وحذفها عند الضرورة
- استخدام إضافات تقلل وتتبع من يجمع البيانات عنا أثناء التصفح

RECIPE
Recentering The Civic Internet
Through Partner Engagement

التعامل مع رسائل البريد الإلكتروني والمرفقات المشبوهة

- لا تفتح رسائل أو مرفقات من مصادر غير موثوقة
- تحقق من الروابط قبل الضغط عليها باستخدام أدوات فحص URL
- في حالة الشك، أرسل الرسالة لقسم الدعم التقني أو استخدم بيئة آمنة لفحصها

نصائح إضافية لبناء الخطة الشخصية

المراجعة الدائمة

الخطة الشخصية للأمان الرقمي هي وثيقة يجب أن تبقى مفتوحة للتغيير والتطوير بناءً على التجربة والتغييرات في بيئة العمل

التثقيف

الاطلاع الدائم على المستجدات التقنية والمخاطر الجديدة المرتبطة ببيئتنا الرقمية، والبحث عن أحدث أساليب الحماية والأدوات الموثوقة

العمل ضمن مجموعة

مشاركة المعارف وأدوات الحماية مع الزملاء والعائلة لبناء بيئة آمنة حولك

طلب الدعم

في حالة وجود خطر أو الشك في سلوك ما، يجب التواصل مع جهة دعم تقني موثوقة

ابق آمنا


RECIPE
Recentering The Civic Internet
Through Partner Engagement