قائمة فحص حماية الهوية الرقمية

هذه القائمة تساعدك على مراجعة وتطبيق خطوات حماية هويتك الرقمية. قم بتحديد المربعات بعد إكمال كل خطوة.

🛡️ أساسيات الحماية

- [ ] استخدم كلمات مرور قوية وفريدة لكل حساب (أكثر من 12 حرفاً، مزيج من الأحرف الكبيرة والصغيرة، الأرقام، والرموز).
- [ ] استخدم مدير كلمات مرور موثوقاً به لتخزين كلمات المرور بأمان.
- [ ] قم بتفعيل التحقق الثنائي (2FA) على جميع حساباتك الهامة (البريد الإلكتروني، وسائل التواصل الاجتماعي، البنوك، إلخ).
- [ ] حافظ على تحديث نظام التشغيل والتطبيقات على جميع أجهزتك بانتظام.
- [ ] استخدم برنامج مكافحة فيروسات موثوقاً به وقم بتحديثه باستمرار.

🌐 التصفح والإنترنت

- [ ] تأكد دائماً من أن المواقع التي تزورها تستخدم اتصالاً آمناً (HTTPS).
- [ ] كن حذراً عند النقر على الروابط أو فتح المرفقات من مصادر غير معروفة أو مشبوهة.
- [ ] استخدم شبكة افتراضية خاصة (VPN) عند الاتصال بشبكات Wi-Fi العامة.
- [ ] تجنب مشاركة المعلومات الشخصية الحساسة على المواقع غير الموثوقة.

📱 حماية الأجهزة المحمولة

- [ ] استخدم قفل شاشة قوي (بصمة الإصبع، التعرف على الوجه، رمز PIN معقد) على هاتفك وجهازك اللوحي.
- [ ] قم بتحميل التطبيقات فقط من المتاجر الرسمية (Google Play Store, Apple App Store).
- [ ] قم بتفعيل خاصية البحث عن الهاتف المفقود/المسروق ومسح البيانات عن بعد.
- [ ] راجع أذونات التطبيقات بانتظام وقم بإلغاء الأذونات غير الضرورية.

👨‍👩‍👧‍👦 حماية الأسرة

- [ ] استخدم أدوات الرقابة الأبوية على أجهزة الأطفال لتحديد المحتوى ووقت الاستخدام.
- [ ] علّم الأطفال أهمية عدم مشاركة المعلومات الشخصية مع الغرباء عبر الإنترنت.
- [ ] ناقش مع كبار السن مخاطر التصيد الاحتيالي والرسائل المشبوهة.
- [ ] راجع إعدادات الخصوصية على حسابات وسائل التواصل الاجتماعي لجميع أفراد الأسرة.

🚨 في حالة التعرض لحادث

- [ ] قم بتغيير كلمات المرور المتأثرة فوراً.
- [ ] أبلغ الجهات المختصة (مثل الشرطة أو وحدة مكافحة الجرائم الإلكترونية) عن الحادث.
- [ ] قم بجمع أكبر قدر ممكن من الأدلة (لقطات شاشة، رسائل، إلخ).
- [ ] استخدم أدوات فحص تسرب البيانات (مثل HaveIBeenPwned) للتحقق مما إذا كانت بياناتك قد تسربت في أي اختراقات سابقة.