Arabic | العربية

Be Connected
Every Australian online.

Australian Government

ملخص العرض التقديمي عبر الإنترنت

إدارة رسائل البريد الإلكتروني الخاصة بك بأمان

امتلاك عنوان بريد إلكتروني هو بوابتك إلى عالم الإنترنت. يسمح لك بالبقاء على تواصل مع العائلة والأصدقاء، والوصول إلى خدمات مثل التسوق عبر الإنترنت والخدمات المصرفية. من المهم الحفاظ على أمان حساب بريدك الإلكتروني قدر الإمكان، باستخدام عبارة مرور قوية ومصادقة متعددة العوامل.

طرق الوصول إلى البريد الإلكتروني

هناك العديد من الطرق للوصول إلى رسائل البريد الإلكتروني الخاصة بك. يمكنك القيام بذلك من خلال:

تطبيق

- استخدام تطبيق موفر خدمة البريد الإلكتروني الذي يمكنك تنزيله من App Store لأجهزة Apple أو متجر Play Store للأجهزة التي تعمل بنظام تشغيل Android
- اربط حساب بريدك الإلكتروني بما يلي:
  - تطبيق البريد المثبت مسبقًا على جهازك الذكي
  - تطبيق البريد أو Outlook على جهاز الكمبيوتر الخاص بك.

الموقع الإلكتروني

- قم بتسجيل الدخول إلى الموقع الإلكتروني الخاص بمزود البريد الإلكتروني الخاص بك من متصفح على جهاز الكمبيوتر أو الجهاز الذكي.

مزودو خدمة البريد الإلكتروني

هناك الكثير من مزودي خدمة البريد الإلكتروني الذين يقدمون خيارات حساب بريد إلكتروني مجاني ومدفوع، بما في ذلك:

Gmail Google

Outlook Microsoft

Yahoo Mail Yahoo

iCloud Apple

ProntonMail Proton AG

تفضل بزيارة موقع Be Connected على الإنترنت للحصول على **أدلة خطوة بخطوة** حول كيفية إعداد Gmail وOutlook وYahoo واستخدامها.

ملاحظة: قد ترغب في إعداد حساب بريد إلكتروني فقط للخدمات المصرفية الخاصة بك أو لاستخدامه فقط للتسوق عبر الإنترنت للمساعدة في إدارة الرسائل الإلكترونية غير المرغوب فيها.

إدارة حساب بريدك الإلكتروني

إعداد المجلدات والتسميات

يعد إعداد المجلدات في صندوق الوارد طريقة رائعة للحفاظ على تنظيم حسابك وتسهيل تحديد موقع رسائل البريد الإلكتروني المهمة عند الحاجة إليها. تسمى المجلدات أحيانًا تسميات، اعتمادًا على خدمة البريد الإلكتروني التي تستخدمها.

تنظيم رسائل البريد الإلكتروني الخاصة بك وحفظها

تحتوي خدمة البريد الإلكتروني الخاصة بك على عناصر تحكم مفيدة تساعدك على حفظ رسائل البريد الإلكتروني بطرق مختلفة وتقلل البريد العشوائي وغير المرغوب فيه إلى الحد الأدنى. عند وصول رسالة بريد إلكتروني جديدة وفتحها لقراءتها، تظهر بعض عناصر التحكم في أعلى الشاشة. يمكنك النقر فوق عناصر التحكم هذه من أجل:

- **الحذف**: نقل البريد الإلكتروني إلى مجلد سلة المهملات
- **الأرشيف**: نقل الرسالة الإلكترونية إلى الأرشيف
- **وضع علامة "غير مقروءة"**: جعل الرسالة الإلكترونية تظهر جديدة مرة أخرى
- **التسميات/المجلد**: قم بتسمية البريد الإلكتروني أو نقله إلى مجلد.

إدارة رسائل البريد الإلكتروني غير المرغوب فيها

تكتشف خدمة البريد الإلكتروني الخاصة بك تلقائيًا رسائل البريد الإلكتروني غير المرغوب فيها المعروفة وتقوم بتحويلها، ولكن لا يزال بإمكان بعض الرسائل غير المرغوب فيها المرور.

إذا كنت تعتبر رسالة بريد إلكتروني في صندوق الوارد عشوائية أو غير مرغوب فيها، يمكنك:

- **الإبلاغ عن محتوى غير مرغوب فيه**: أخبر موفر خدمة البريد الإلكتروني أن الرسالة الإلكترونية غير مرغوب فيها
- **حظر الرسائل الإلكترونية**: إيقاف تلقي الرسائل الإلكترونية من المرسل
- **إلغاء الاشتراك**: توقف عن تلقي الرسائل الإخبارية أو رسائل البريد الإلكتروني التسويقية التي اشتركت فيها.

إذا كنت تعتقد أنك ألغيت الاشتراك ولكنك لا تزال تتلقى رسائل بريد إلكتروني غير مرغوب فيها، فيمكنك تقديم شكوى إلى **هيئة الاتصالات والإعلام الأسترالية Australian Communications and Media Authority**.

نصيحة: لتجنب رسائل البريد الإلكتروني غير المرغوب فيها، كن حذرًا من تقديم معلوماتك للمسابقات وأي مربعات محددة مسبقًا لتلقي رسائل بريد إلكتروني تسويقية عند شراء منتجات أو خدمات.

حافظ على أمان حساب بريدك الإلكتروني

عبارات المرور

حافظ على أمان حساباتك باستخدام عبارات مرور قوية. عبارات المرور هي الإصدار الأكثر أمانًا من كلمات المرور وتتكون من أربع كلمات عشوائية أو أكثر.

حاول التفكير في عبارة مرور مختلفة لكل حساب من حساباتك ولا تعيد تدوير أجزاء من أي عبارات مرور قديمة.

عند اختيار عبارة المرور الخاصة بك، اجعلها:

- **طويلة** - 14 حرفًا على الأقل
- **لا يمكن التنبؤ بها** - استخدم أربع كلمات عشوائية أو أكثر بأرقام ورموز وأحرف كبيرة وصغيرة
- **فريدة** - لا تعيد استخدام عبارات المرور الخاصة بك.

على سبيل المثال، أصفر لذا مرحبًا نبات <
*Yell*w-S0heyPl@nt!*

نصيحة: يمكن أن يساعدك تطبيق إدارة كلمات المرور أيضًا في إنشاء وتخزين عبارات مرور معقدة يصعب على الآخرين تخمينها أو اختراقها. يمكنك العثور على معلومات حول تطبيقات **إدارة كلمات المرور** وكيفية إعدادها على موقع Be Connected.

استخدم اتصال آمن

عندما تحتاج إلى الوصول إلى حساباتك أو إرسال معلومات حساسة أو إدخال كلمات مرور، اتصل بشبكة إنترنت موثوق بها، مثل شبكة المنزل أو العمل أو باستخدام شبكة إنترنت الجوال الخاص بك إذا كانت متوفرة. شبكة الواي فاي العامة ليست آمنة مثل شبكة الواي فاي في المنزل أو العمل.

خيارات استرداد الحساب

تأكد من إعداد رقم هاتف مخصص لاسترداد الحساب أو عنوان بريد إلكتروني بديل لجميع حسابات بريدك الإلكتروني. إذا فقدت الوصول إلى حسابك، أو تم اختراقه، فيمكنك إعادة تعيين كلمة المرور باستخدام خيار الاسترداد.

المصادقة متعددة العوامل

من الجيد دائمًا تشغيل المصادقة متعددة العوامل لحساباتك. تضيف المصادقة متعددة العوامل (المعروفة أيضًا باسم المصادقة ذات الخطوتين) طبقة إضافية من الأمان. هذا يعني أنه عند تسجيل الدخول إلى حساب باستخدام كلمة المرور الخاصة بك، قد يُطلب منك القيام بخطوة إضافية لتأكيد هويتك - مثل إدخال رمز من رسالة نصية أو استخدام تعريف التعرف على الوجه.

استخدم أمان الجهاز

يعد استخدام برامج الأمان على جهاز الكمبيوتر الخاص بك أحد أبسط الطرق لتأمين حساباتك وأجهزتك. يتضمن الأمان الجيد للكمبيوتر تثبيت برامج مكافحة التجسس وبرامج مكافحة الفيروسات وبرامج جدار الحماية ذات السمعة الطيبة. يجب عليك أيضًا تحديث أدوات وتطبيقات الأمان عبر الإنترنت من خلال تمكين التحديثات التلقائية.

رسائل البريد الإلكتروني الاحتيالية

تم تصميم رسائل البريد الإلكتروني الاحتيالية لتبدو وكأنها من مؤسسات شرعية تعرفها. قد تبدو حقيقية، باستخدام شعارات وعنوان بريد إلكتروني مشابه للمؤسسة التي ينتحلون شخصيتها. يمكن أن تبدو رسائل البريد الإلكتروني الاحتيالية وكأنها من البنك الذي تتعامل معه أو مزود خدمة الإنترنت أو وكالة حكومية أو بائع تجزئة أو حتى محتال يتظاهر بأنه صديق أو أحد أفراد الأسرة. من خلال التظاهر بأنها من شخص تثق به، يستخدم المحتالون الشعور بالإلحاح لخداعك لدفع الأموال أو تقديم معلومات شخصية، مثل كلمات المرور المهمة أو بطاقة الائتمان أو التفاصيل المصرفية.

تسمى هذه الأنواع من عمليات الاحتيال بعمليات احتيال انتحال الهوية أو رسائل البريد الإلكتروني للتصيد الاحتيالي.

نصائح لتجنب رسائل البريد الإلكتروني الاحتيالية

- ابحث عن علامات البريد الإلكتروني الاحتيالي. يمكن لرسائل البريد الإلكتروني الاحتيالية:
  - أن تخلق شعورًا بالإلحاح أو تستخدم أساليب التخويف، أو المطالبة بالدفع أو مطالبتك بتأكيد البيانات الشخصية
  - استخدام تحيات عامة مثل "عزيزي العميل" أو "عزيزي المستخدم" أو عدم التحية على الإطلاق
  - أن تطلب منك النقر فوق رابط أو تنزيل ملف قد يوجهك إلى موقع إلكتروني مزيف أو يحتوي على فيروس أو برامج ضارة.
- تحقق دائمًا من أن عنوان البريد الإلكتروني للمرسل شرعي واتصل بالمنظمة مباشرة من خلال البحث عن الموقع الإلكتروني الرسمي ورقم الهاتف.
- لا تقم أبدًا بتسجيل الدخول إلى حساباتك عبر الإنترنت أو التحقق من التفاصيل عبر رابط في رسالة بريد إلكتروني أو النقر فوق الروابط أو فتح المرفقات في رسائل البريد الإلكتروني من مرسلين غير معروفين أو مشبوهين.
- احذف رسائل البريد الإلكتروني المشبوهة أو الاحتيالية المحتملة، واستخدم خيار "الإبلاغ عن البريد العشوائي" لتصنيفها على أنها بريد إلكتروني غير مرغوب فيه.

نصيحة: إذا شعرت بالارتياب حيال رسالة بريد إلكتروني، تحدث إلى صديق موثوق به أو أحد أفراد العائلة واتصل بالمؤسسة باستخدام رقم الهاتف الموجود على الموقع الإلكتروني الخاص بها.

قم بزيارة موقع Be Connected للحصول على **دليل عمليات احتيال** انتحال الهوية المجاني الذي تم تطويره باستخدام Scamwatch.

خذ الوقت الكافي لاكتشاف Be Connected

Be Connected هو موقع إلكتروني شامل يحتوي على موارد مجانية مصممة خصيصًا لدعم كبار السن الأستراليين للاتصال بأمان عبر الإنترنت والتنقل في العالم الرقمي بثقة. الموقع مفيد أيضًا للعائلات والمنظمات المجتمعية التي ترغب في مساعدة أفراد المجتمع الأكبر سنًا في الوصول إلى جميع مزايا الإنترنت.

تفضل بزيارة beconnected.esafety.gov.au

تم تطوير هذا البرنامج من قبل "مفوض السلامة الإلكترونية" eSafety Commissioner كجزء من مبادرة Be Connected.

eSafety Commissioner

Australian Government