



دليل الممارسات السيبرانية الآمنة في بيئة العمل

كن واعياً.. لتكن آمناً

Cybersecurity@ibnsina.edu.sa

المحتويات

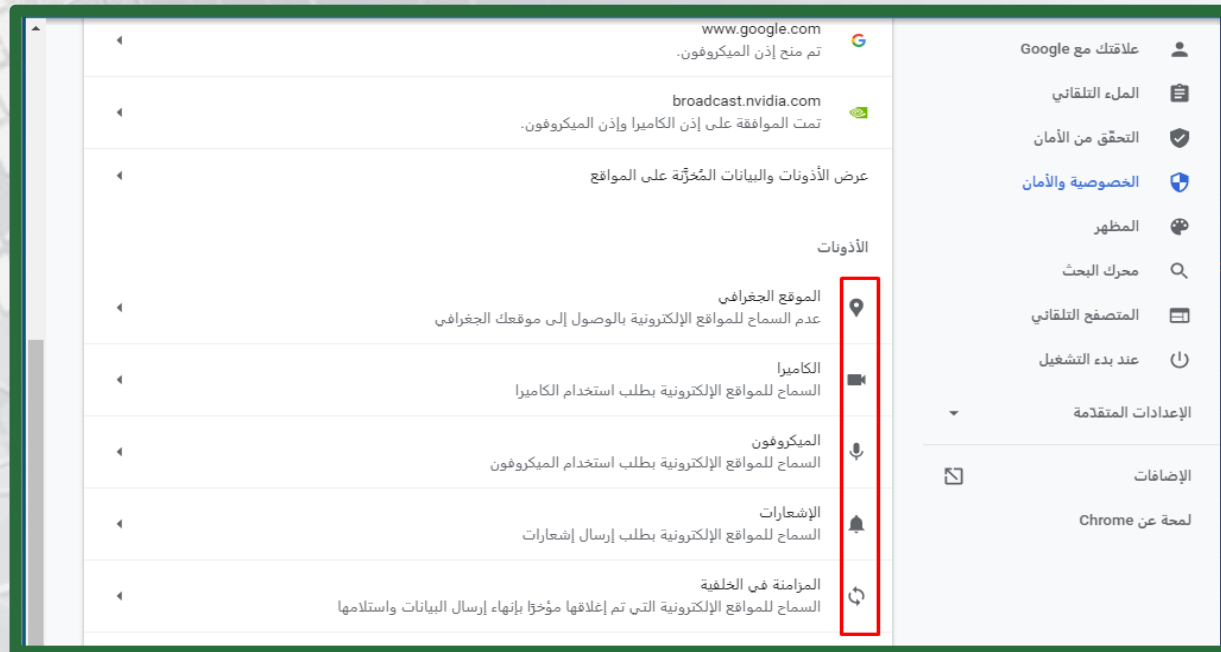
- ٣ التعامل الآمن مع خدمات تصفح الإنترنت
- ٦ التعامل الآمن مع خدمات البريد الإلكتروني
- ٨ التعامل الآمن مع وسائل التواصل الاجتماعي
- ٩ الاستخدام الآمن للأجهزة المحمولة ووسائط التخزين الخارجية

التعامل الآمن مع خدمات تصفح الإنترنت

١- تجنب زيارة المواقع المشبوهة وتتاكد من وجود رمز الأمان HTTPS.



٢ - قيد الوصول إلى الموقع الجغرافي والكاميرا والميكروفون:



التعامل الآمن مع خدمات تصفح الإنترنت



٣ - إيقاف التنزيلات التلقائية:

The screenshot shows the Chrome settings page with the 'Advanced' section expanded. The 'Autoplay' section is highlighted with a red box, and the 'Downloads' section is also highlighted with a red box. The 'Downloads' section includes the option 'Allow automatic downloads' which is currently turned on.

الأذونات	علاقتك مع Google
الموقع الجغرافي عدم السماح للمواقع الإلكترونية بالوصول إلى موقعك الجغرافي	علاقتك مع Google الملء التلقائي
الكاميرا السماح للمواقع الإلكترونية بطلب استخدام الكاميرا	التحقق من الأمان الخصوصية والأمان
الميكروفون السماح للمواقع الإلكترونية بطلب استخدام الميكروفون	المظهر
الإشعارات السماح للمواقع الإلكترونية بطلب إرسال إشعارات	محرك البحث
المزامنة في الخلفية السماح للمواقع الإلكترونية التي تم إغلاقها مؤخراً بإنهاء إرسال البيانات واستلامها	المتصفح التلقائي
أذونات إضافية	عند بدء التشغيل
مستشعرات الحركة السماح للمواقع الإلكترونية باستخدام مستشعرات الحركة	الإعدادات المتقدمة
عمليات التنزيل التلقائية السماح للمواقع الإلكترونية بطلب تنزيل الملفات المتعددة تلقائياً	الإضافات
معالجات البروتوكول السماح للمواقع الإلكترونية بطلب معالجة البروتوكولات	لمحة عن Chrome
أجهزة MIDI السماح للمواقع الإلكترونية بطلب الاتصال بأجهزة MIDI	
أجهزة USB السماح للمواقع الإلكترونية بطلب الاتصال بأجهزة USB	
المنافذ التسلسلية السماح للمواقع الإلكترونية بطلب الاتصال بمنافذ تسلسلية	
تعديل الملف السماح للمواقع الإلكترونية بطلب تعديل الملفات والمجلدات على جهازك	

التعامل الآمن مع خدمات تصفح الإنترنت



- ٤ - لا تستخدم خاصية الدخول التلقائي.
- ٥ - قم بمسح المحفوظات والملفات المؤقتة بشكل دوري من المتصفح.
- ٦ - استخدم أحدث إصدار من برنامج متصفح الإنترنت.
- ٧ - تأكد من ضبط إعدادات الأمان والخصوصية لمتصفح الإنترنت.
- ٨ - امنع النوافذ المنبثقة، فقد تؤدي إلى هجمات خبيثة أو خفية.



التعامل الآمن مع خدمات البريد الإلكتروني

خصوصاً مع رسائل التصيد الإلكتروني



ما هو التصيد الإلكتروني؟

هو طريقة خطيرة وفعالة لعمليات الاختراق. يتظاهر المجرمون بأنهم أشخاص معروفين، ويقوموا بإرسال رسائل للمستهدفين تتضمن رابطاً أو مرفقاً ضاراً. ويكون الهدف من ذلك أن ينقر المستهدفون على الرابط، وهو ما قد يقوم بتنزيل برنامج ضار أو يقودهم إلى موقع غير موثوقة لسرقة معلوماتهم الشخصية.

علامات قد تدل على أن البريد تصيدي:

- مرسلون غير معتادين يطلبون بياناتك الشخصية.
- تغيير بسيط في ترتيب الأحرف لعنوان مستخدم تعرفه.
- أخطاء إملائية أو نحوية.
- مجالات بريد إلكتروني غير متوقعة.
- طلب الرد بشكل عاجل على المحتوى المرسل أو التهديد.

التعامل الآمن مع خدمات البريد الإلكتروني

خصوصًا مع رسائل التصيد الإلكتروني



طرق الوقاية من هجمات التصيد الإلكتروني:

- تجنب فتح رسائل البريد الإلكتروني من المصادر غير الموثوقة.
- تحقق من المرسل قبل أن تنقر على أي رابط أو مرفق.
- تأكد قبل الرد على أي رسائل تطلب منك معلومات شخصية.
- عند تلقيك لرسائل تطلب تحديث بياناتك، قم بالتحديث عبر الموقع الإلكتروني فقط وليس عبر الرابط المرفق.
- لا تشارك في العروض الترويجية باستخدام البريد الإلكتروني الرسمي الخاص بجهة عملك.
- إذا كانت الرسالة المشبوهة تبدو وكأنها رسالة من شخص تعرفه، فتواصل مع هذا الشخص عبر وسيلة اتصال مختلفة، للتأكد من أنها آمنة.
- ثبت جميع تحديثات البرامج والأنظمة على جهازك.

التعامل الآمن مع وسائل التواصل الاجتماعي



- استخدم كلمات مرور قوية لحساباتك عبر مواقع التواصل الاجتماعي.
- قم بتفعيل خاصية التحقق الثنائي في مواقع التواصل الاجتماعي.
- لا تقم بنشر المعلومات الحساسة أو المعلومات الوظيفية عبر مواقع التواصل الاجتماعي.
- لا تستخدم مواقع التواصل الاجتماعي لتبادل الوثائق أو البيانات الخاصة بالعمل.
- تجنب تسجيل الدخول على مواقع التواصل الاجتماعي باستخدام أجهزة أو شبكات عامة.
- قم بتفعيل وتحديث الأسئلة الأمنية بشكل دائم، واحفظها في مكان آمن.
- قم بتثبيت التحديثات الأمنية والإصلاحات لتطبيقات التواصل الاجتماعي من مصادر موثوقة فور صدورها.

**تذكر جيدا " أن ما تنشره مرة واحدة على الأنترنت..
سيظل دوماً على الإنترنت " ..**

الاستخدام الآمن للأجهزة المحمولة ووسائط التخزين الخارجية



- قم بتثبيت التحديثات الأمنية والإصلاحات لأنظمة التشغيل والبرامج والتطبيقات من مصادر موثوقة فور صدورها.
- قم بإنشاء كلمة مرور معقدة على الأجهزة، ولا تشاركها مع أحد.
- لا تستخدم وسائط التخزين الخارجية على أجهزة العمل.
- لا تقم بتوصيل أي وسائط تخزين غير آمنة أو غير معروفة بجهازك.
- تأكد دائما من فحص وسائط التخزين الموثوقة والمعروفة المصدر قبل فتحها.
- قم بحذف ملفات التخزين المؤقتة "Cookies" بشكل دوري.
- تأكد من تثبيت وتفعيل برامج مكافحة الفيروسات على جهازك.