دليل الممارسات السيبرانية الآمنة في بيئة العمل

كن واعيًا.. لتكن آمنًا

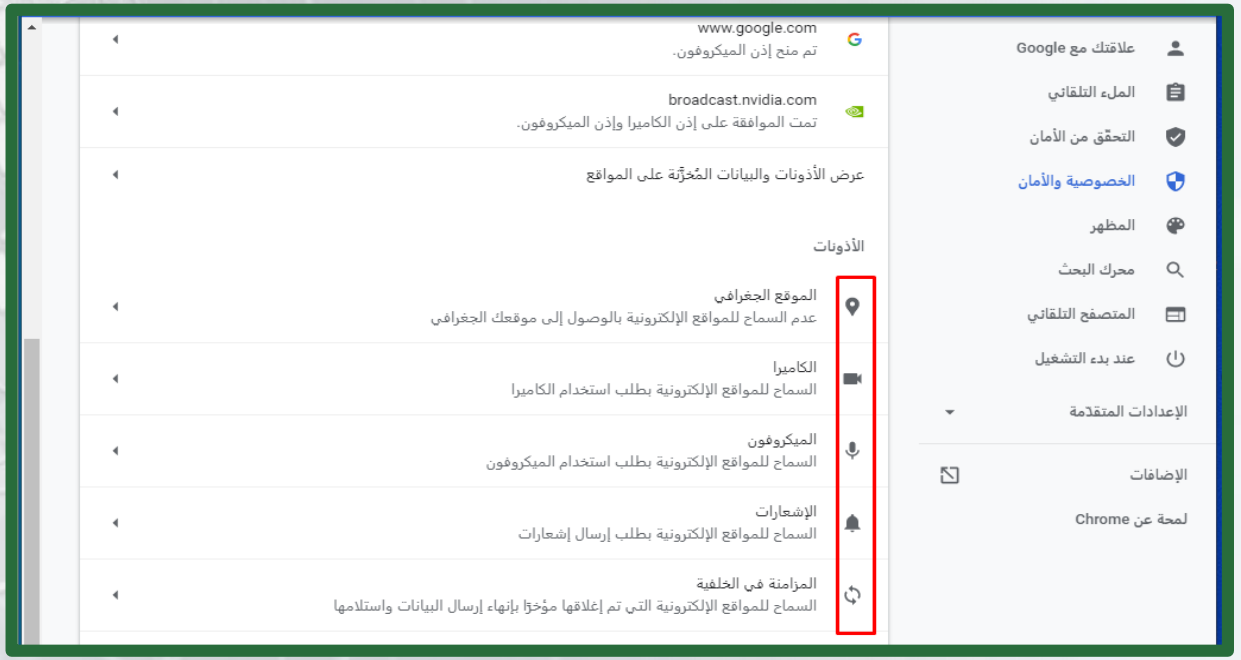
Cybersecurity@ibnsina.edu.sa

المحتويات

التعامل الآمن مع خدمات تصفح الإنترنت

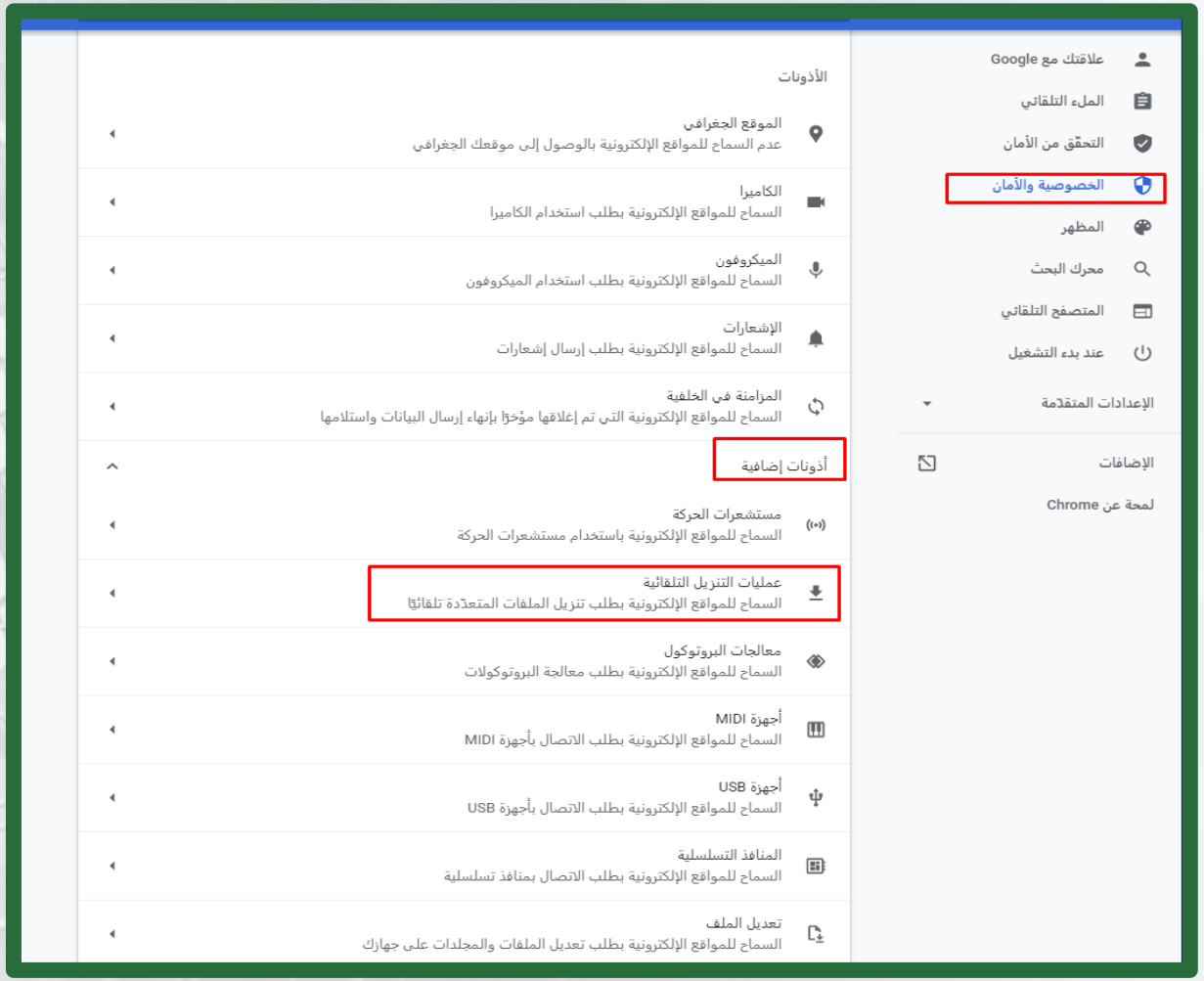
١ـ تجنب زيارة المواقع المشبوهة وتتأكد من وجود رمز الأمان HTTPS.

٢ ـ قيد الوصول إلى الموقع الجغرافي والكاميرا والميكروفون:



التعامل الآمن مع خدمات تصفح الإنترنت

٣ ـ إيقاف التنزيلات التلقائية:



التعامل الآمن مع خدمات تصفح الإنترنت

٤ – لا تستخدم خاصية الدخول التلقائي.

٥ ـ قم بمسح المحفوظات والملفات المؤقتة بشكل دوري من المتصفح.

٦ ـ استخدم أحدث إصدار من برنامج متصف الإنترنت.

٧ ـ تأكد من ضبط إعدادات الأمان والخصوصة لمتصف الإنترنت.

٨ ـ امنع النوافذ المنبثقة، فقد تؤدي إلى هجمات خبيثة أو خفية.

التعامل الآمن مع خدمات البريد الإلكتروني

خصوصًا مع رسائل التصيد الإلكتروني

ماهو التصيد الإلكتروني؟

هو طريقة خطرة 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 الاحرف 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 رلاسائل 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 مرسلة 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 دومًا على الإتنترنت "..

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.