CITRA
الهيئة العامة للاتصالات وتقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

توصيات للحد من اختراق أجهزة المحمول

البيانات الشخصية بالمحمول مستهدفة ويقع على صاحب البيانات مسوؤلية اتباع التوصيات الأمنية لحماية بياناته الشخصية من الاختراق والسرقة.

شبكة WiFi

- قم بتعطيل خاصية التشغيل التلقائي إلى الشبكات العامة.
- في حالة عدم استخدام شبكة WiFi قم بتعطيلها.
- تأكد من إرسال البيانات الحساسة عبر شبكة WiFi آمنه و موثوقة.

التطبيقات

- قم بتحميل التطبيقات المتاحة بالمتجر الرسمي الخاص بجهازك، ولا تقم بتحميل أي تطبيق مباشرة من المتصفح.
- راجع تقييم التطبيق قبل تحميلة خصوصا اذا كان مجهولة المصدر.
- قم بتحديث التطبيقات بشكل دوري لضمان الأمان.
- احذف التطبيق إذا لم يعد مدعوما من متجرك.
- لا تفرط في منح الصلاحيات إلى التطبيقات.
- قم بتحميل أحد تطبيقات المضادة للفيروسات antivirus للتأكد من سلامة جهازك من أي تهديد.

التصيد الاحتيالي الصوتي (عبر الصوت)

- لا تفصح عن معلوماتك الشخصية والمالية لأية مكالمة مجهولة المصدر .
- تحقق من هوية المتصل أولا.
- إذا كان الاتصال مشبوه، قم بإبلاغ مركز عملاء المؤسسة المعنية.

خاصية Bluetooth

- عليك تعطيل خاصية التشغيل التلقائي للـ Bluetooth.
- يجب استخدامها فقط عند الحاجة لها.

المتصفح

- احذر من الإعلانات فغالبا ما تؤدي إلى مواقع احتيالية.
- تفحص العناوين والروابط الإلكترونية، ابحث دائما عن https، وتأكد من صحة تهجئة العناوين والروابط الإلكترونية.
- لا تحتفظ مطلقا بمعلومات تسجيل الدخول عند استخدام اية متصفح.

التصيد الاحتيالي (عبر الرسائل القصيرة)

- لا تقم بالكشف عن معلوماتك الشخصية عندما يكون مصدر الرسالة غير معروف.
- احذر من الرسائل الاحتيالية المماثلة في بعض منصات التواصل الاجتماعي مثل الواتس آب، الانستغرام، الفيس بوك ماسنجر، وسناب جات وغيرها.
- تعامل مع الرسائل ذات المصدر الغير معروف بمبدأ فكر قبل أن تضغط!

@CitraKuwait
@CitraKuwait
www.citra.gov.kw
ncsc@citra.gov.kw