



سايبر كيدز  
CyberKids

جمعية الأمن السيبراني للأطفال  
Cyber Security for Children Association

جمعية أهلية معتمدة برقم ١٥٥٧

## الرؤية

نحو مجتمع آمن لأطفالنا

## الرسالة

المساهمة في بناء جيل مثقف سيبرانياً وتقديم النصح والارشادات اللازمة التي تساهم في توفير بيئة آمنة مطمئنة للأطفال

## أهداف الجمعية

- المساهمة في رفع مستوى وعي الأطفال وذويهم ضد المخاطر السيبرانية
- تطوير مهارات الحماية والأمان لدى الأطفال في مجال الحماية والأمان
- المساهمة في تدريب الأطفال حول الاستخدام الآمن للإنترنت
- تقديم النصح والإرشادات في الأمن السيبراني للأطفال

جمعية الأمن السيبراني للأطفال  
Cyber Security for Children Association



# دورة الأمن السيبراني للأطفال

الفئة المستهدفة من ١٣-١٦ سنة



# حماية جهازك

كن آمنًا



مقدم الدورة/ فراس بن عبدالعزيز الصحن

## حماية جهازك

كن آمنا



### حماية الاجهزة والبيانات:

عبارة عن توفير الأدوات والوسائل والتطبيقات اللازمة لحماية الأجهزة والبيانات من المخاطر التي تهددها سواء كانت هجمات داخلية أو خارجية.

### أنواع الهجمات التي تهدد أمان الأجهزة :

- هجمات فيروسية
- اختراقات أمنية





## الفيروسات :

هي برمجيات ضارة يتم تحميلها على كمبيوتر المستخدم دون علم المستخدم بها، وتقوم بتنفيذ إجراءات ضارة؛ فالفيروس يقوم بالتكرار الذاتي عن طريق نسخ نفسه إلى برنامج آخر

## الاختراقات الأمنية:

هو الدخول بطريقة غير مشروعة إلى الحاسب أو الشبكة عن طريق ثغرة في النظام ، ويلجأ المُخترِق (Hacker) عادةً إلى أساليب لتعديل النظام وخصائصه الأمنية من أجل تسهيل وصوله إليه؛ وذلك تبعاً لنوع النظام والهدف الذي استُخدم له.



# كيف جهازك يكون آمن ؟

## ١- الحذر الشخصي :

يُعدّ الحذر الشخصي أول طبقة من طبقات الحماية ضد البرامج الضارة ، ومنها :

- رسائل التصيد الاحتيالي Phishing
- الهندسة الاجتماعية Social Engineering
- الحذر من المواقع والتطبيقات غير الموثوقة
- الحذر من الاتصال بالشبكات المجهولة والغير آمنة
- تفعيل الجدار الناري Firewall والتحديث باستمرار

## PHISHING



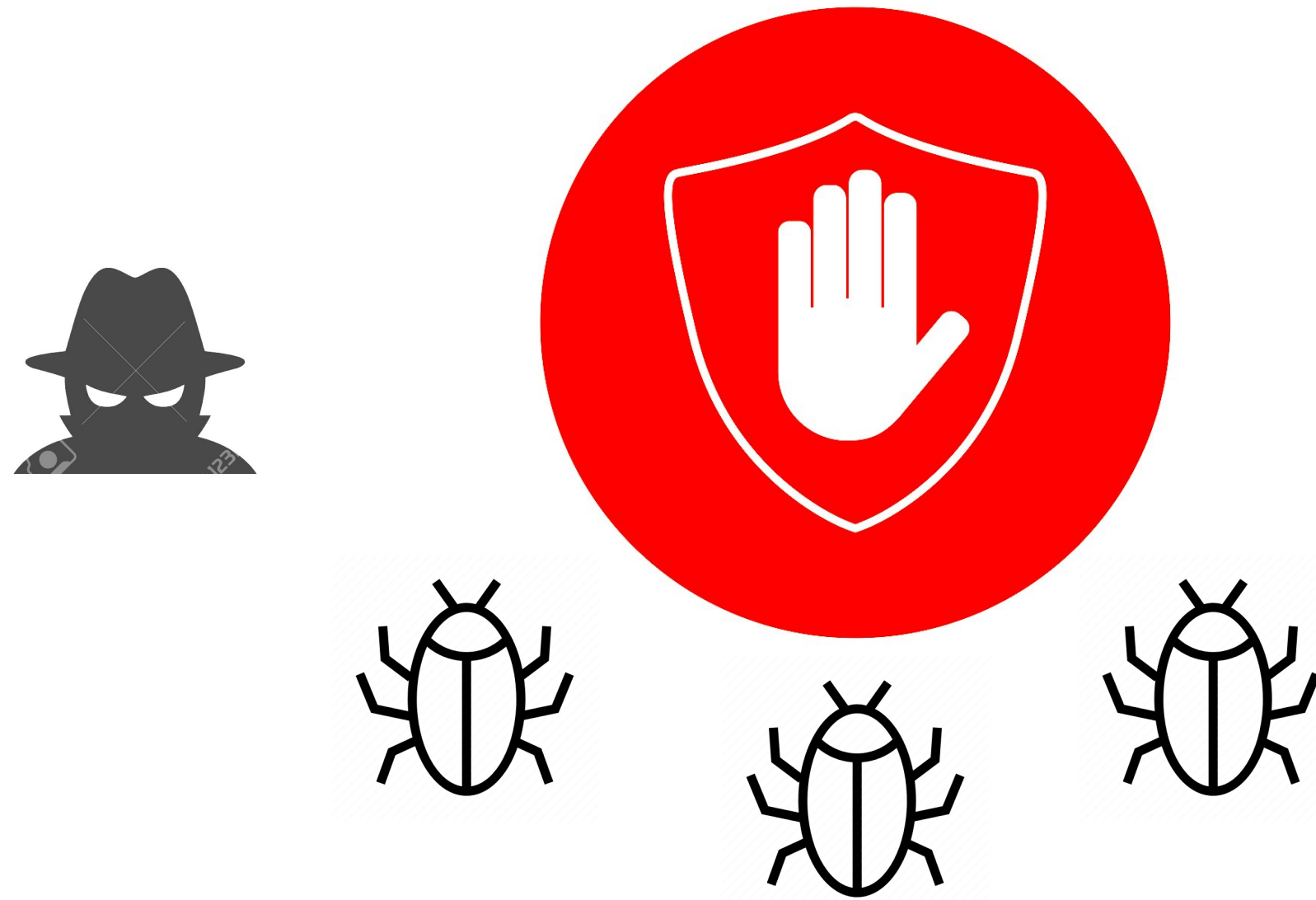




## ٢ - أدوات الحماية

توفر برامج الحماية من البرمجيات الضارة طبقة الحماية الثانية الضرورية لجهازك وشبكتك ، ويتم من خلالها فحص الجهاز بشكل دوري للكشف عن تسلل أي برنامج ضار إليه وإزالته والتحذير من مواقع الويب المشبوهة إن إمكانية توفير حماية تامة شبه مستحيلة. ولكن من شأن الحذر الشخصي وأدوات الحماية الفعالة الحفاظ على سلامة جهازك قدر الإمكان.

**من أهم برامج الحماية التي توفر حماية للجهاز وللشبكة وتصفح آمن عن طريق VPN مع أدوات حماية كلمات المرور**



- برنامج Norton Antivirus Basic by Symantec
- برنامج McAfee Total Protection
- برنامج Bitdefender Total Security
- برنامج Kaspersky Internet Security
- برنامج TOTALAV Security Suite
- برنامج Malwarebytes

اختبار موقع غير آمن



🔒 wicar.org

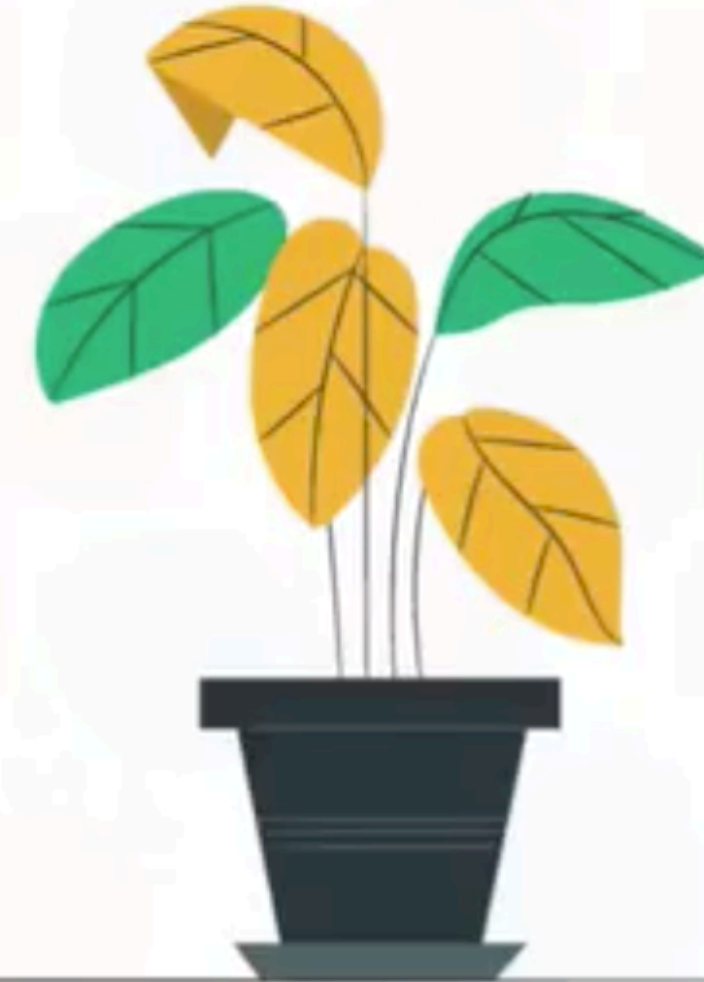
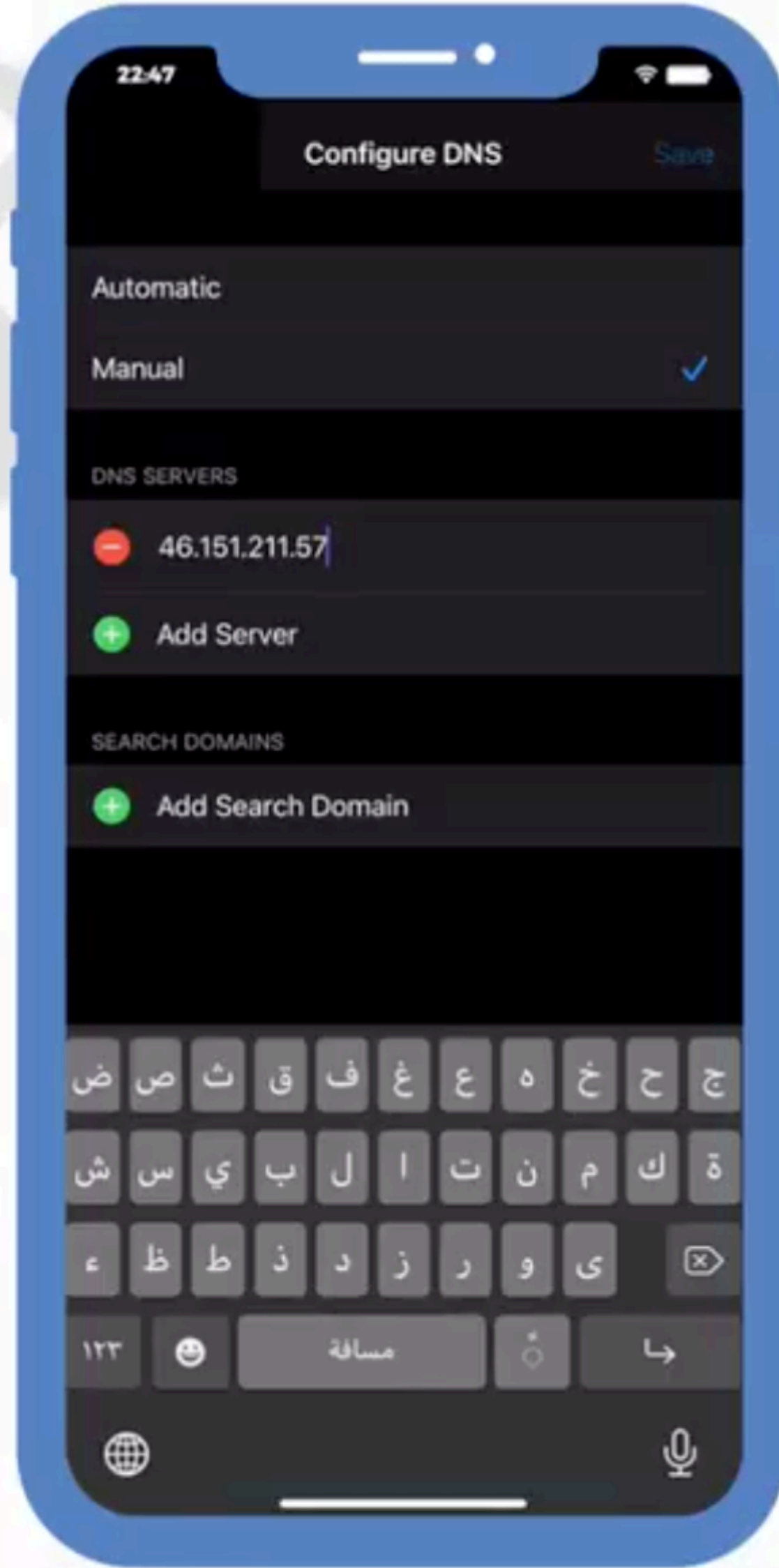
AA



سایبرکیدز  
CyberKids



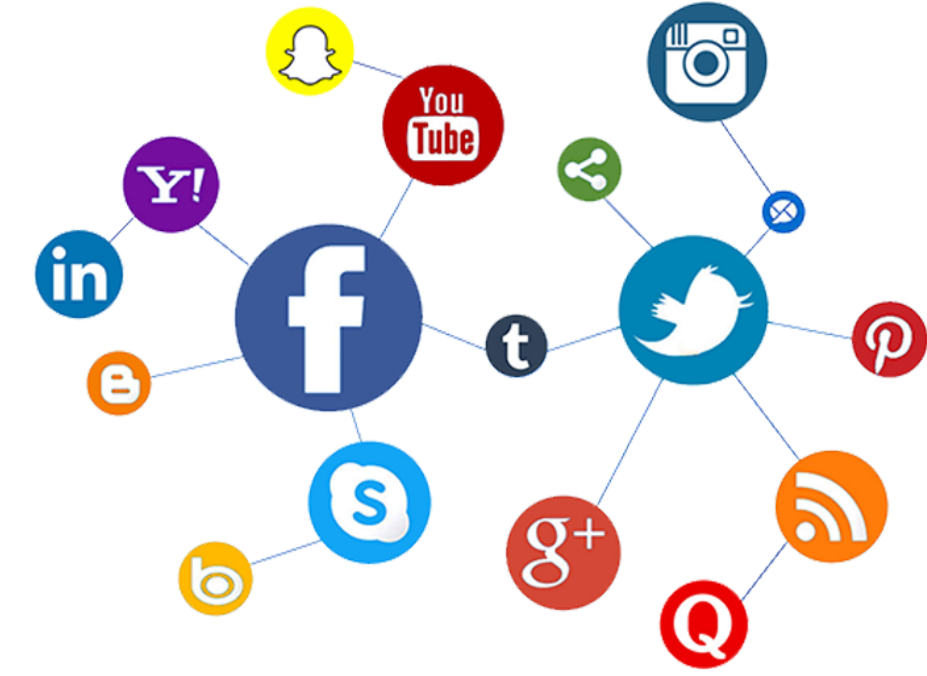
46.151.211.57



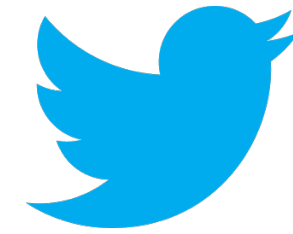




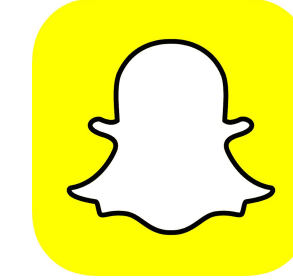
# حماية حساباتك



- Settings
- Security
- Two-Factor Authentication
- Text Message
- أدخل رقم هاتفك
- أدخل رمز التأكيد



- الإعدادات والخصوصية
- الحساب
- الأمان
- المصادقة بعاملين
- تفعيل الرسالة النصية
- البدء وادخل كلمة المرور
- أدخل رقم هاتفك
- أدخل رمز التأكيد

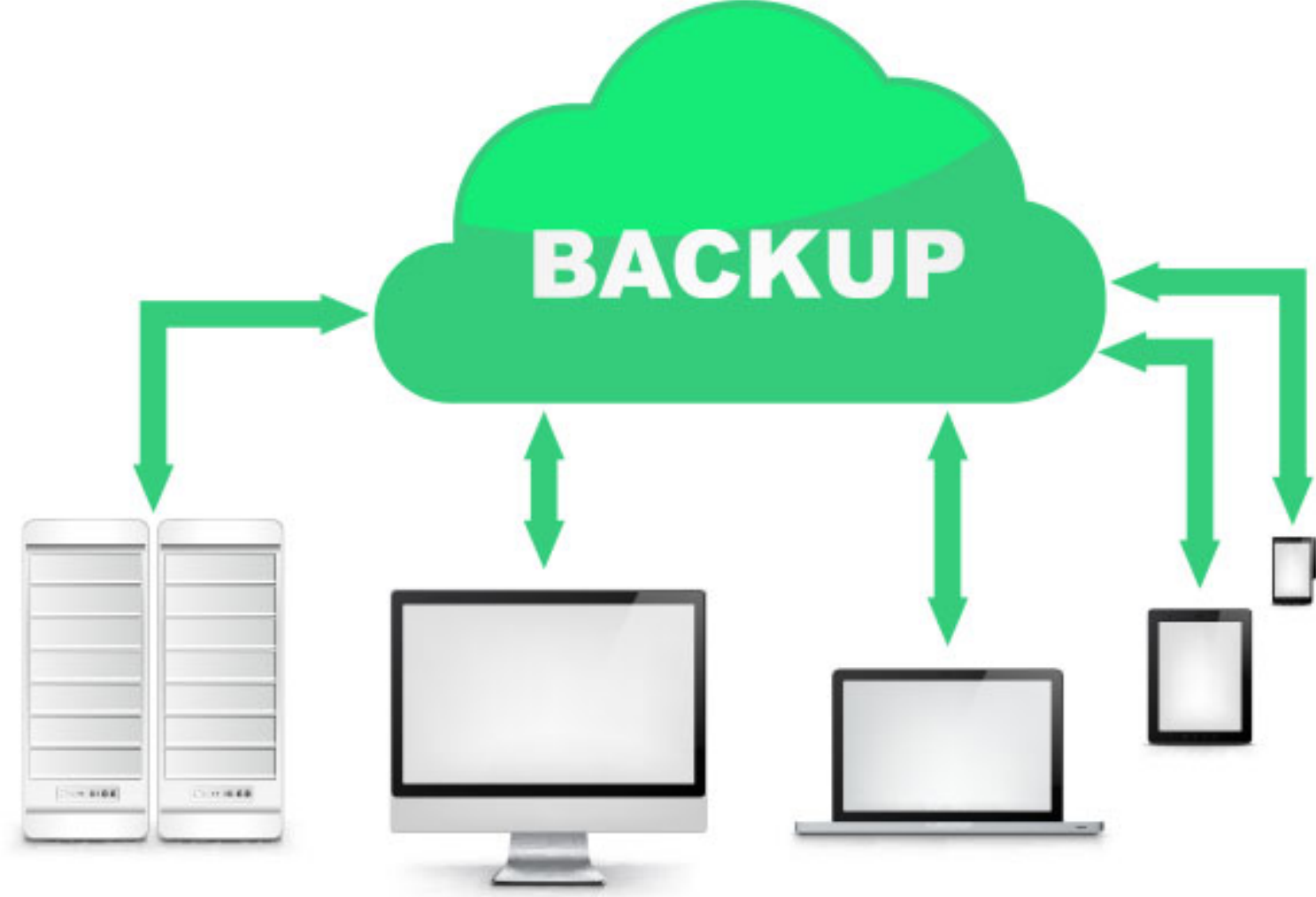


- الإعدادات
- تسجيل الدخول بخطوتين
- متابعة
- التحقق برسالة نصية
- أدخل الرمز المرسل لك



- الإعدادات
- الحساب
- التحقق بخطوتين
- تمكين
- أدخل الرقم السري وقم بتأكيده
- أدخل البريد الإلكتروني وقم بتأكيده

# توصيات لحماية حمايتك

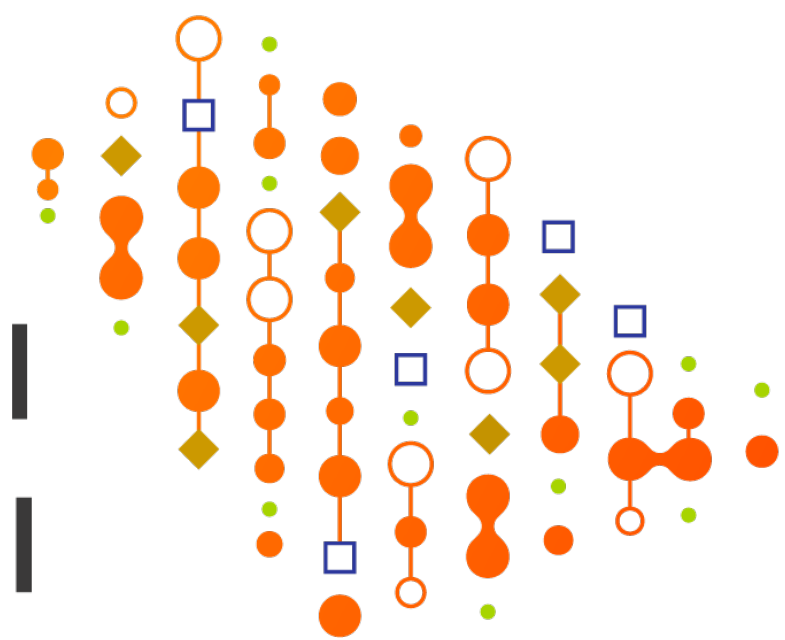


- الاحتفاظ بنسخة احتياطية لبياناتك
- عدم مشاركة معلوماتك الشخصية مع مجهولين
- اختيار كلمة سر قوية ومختلفة لكل حساب
- تغيير كلمات المرور بشكل دوري يقلل من خطر تعرضها للاختراق
- إيقاف تشغيل Wi-Fi و Bluetooth عند عدم الحاجة لها
- تحميل التطبيقات من المواقع الموثوقة والمتاجر الرسمية App Store و Google play
- التأكد من أذونات التطبيقات وسياسة الخصوصية قبل استخدامها
- تأمين حساباتك عن طريق التحقق بخطوتين
- تأمين الشبكة اللاسلكية بتشفير WPA2
- الحذر من حفظ البيانات الخاصة على أجهزة متصلة بالإنترنت.
- الحذر من الروابط المنبثقة pop up
- الحذر من نشر معلومات خاصة على شبكات التواصل الاجتماعي.
- الحذر الدائم عند فتح مرفقات البريد الإلكتروني او الروابط على الانترنت.
- عدم استخدام الشبكات اللاسلكية العامة والغير امنه.
- استخدام برامج الحماية والتأكد من تحديث قاعدة بياناتها.
- الحذر قبل وصل أي جهاز خارجي بالأجهزة الشخصية.
- الحذر من هجمات الهندسة الاجتماعية.
- مراقبة الحسابات والأجهزة الخاصة وملاحظة النشاطات الغير اعتيادية.
- عدم ترك الأجهزة الشخصية بدون رقابة.

سايبر كيدز  
CyberKids

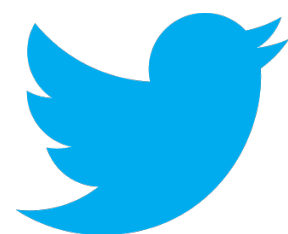
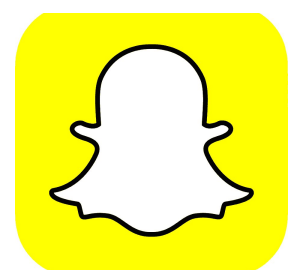


العطاء الرقمي  
Attaa Digital

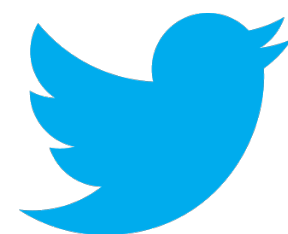


تتكرراً لكم..

cyberkidsorg



@FIRASNSY



info@cyberkids.org.sa

