



يعد "سكايب" من أكثر البرامج التي استخدمها السوريون خلال الثورة السورية، إذ يسمح بإجراء محادثات صوت وصورة عبر الإنترنت، ويعود كثرة استخدامه إلى ما يشاع عن أمانه وحماية مستخدمه.

لكن البرنامج بنظر الخبراء ليس آمناً بشكل كامل، ورغم إجراءات الخصوصية والأمان التي يوفرها مزود الخدمة، إلا أن محادثات "سكايب" تبقى عرضة للمراقبة من أطراف خارجية قد ترغب بالتلصص على محادثاتنا، لذلك يُنصح باتباع بعض الإجراءات التي تجعله أكثر أماناً.

بداية، **يبنفي تحديث نظام التشغيل والبرامج بشكل دوري لحماية حواسيبنا من الإصابة بالبرمجيات الخبيثة.**

- استخدام برنامج مضاد للفيروسات مثل برنامج آفيرا بشكل دائم للحماية من البرمجيات الخبيثة، وهو مضاد للفيروسات موثوق ومجاني ينصح باستخدامه في سوريا، ويمكن تحميله من موقعه الرسمي.

- الحصول على برنامج "سكايب" من موقع موثوق للتأكد من عدم احتوائه على برمجيات خبيثة قد تحوي برامج تجسس تؤدي للتلصص على محادثاتنا، وبما أن خدمة سكايب مجوية بسوريا يمكننا تحميله من هنا:

سكايب من أجل وندوز : سكايب من أجل وندوز (link is external)

سكايب من أجل ماك : سكايب من أجل ماك (link is external)

- استخدام كلمة سر قوية، ك استخدام حروف وأرقام ورموز عشوائية لحماية معلوماتنا ومنع المتلصصين من الوصول إليها. ولا نشارك كلمة السر الخاصة بنا مع أي طرف آخر ونقم بتبديلها دوريًا.

- ضبط إعدادات الخصوصية سكايب إلى أقصى درجات الآمان، من القائمة الرئيسية في سكايب نذهب إلى خصوصية ونضبط الإعدادات على النحو التالي:

السماح بمحادثات من الأشخاص في قائمة جهات الإتصال فقط

استلام الفيديو ومشاركة الشاشة تلقائياً من جهات الإتصال فقط

- مسح المحادثات السابقة ونطلب من أصدقائنا مسح نص المحادثات دائماً.
- استخدام شبكة افتراضية موثوقة لتشفيр إتصالتنا بالإنترنت والابتعاد عن الرقابة وينصح باستخدام "في بي إن" عند استخدامنا "سكايب" في سوريا.
- التأكد من شخصية محدثنا على الطرف الآخر بالتأكد من الصوت أو عبر أسئلة أمان مشتركة.
- عدم الضغط على أية روابط أو مرفقات بدون التأكد من مصدرها فقد تكون ملفات تحوي برامج خبيثة.

مشروع سلامتك – السورية نت

المصادر: