Veilig internetten.nl

5 نصائح أساسية للبقاء آمنًا ومستمتعًا أثناء وجودك في عالم الإنترنت

الإنترنت، هذا العالم المتصل الذي يمتد إلى كل ركن من أركان حياتنا، حيث يُمنحنا مجموعة واسعة من التطبيقات والتقنيات التي تجعل الحياة أسهل وأكثر متعة. فيتيح لنا التواصل الفعّال عبر الرسائل الإلكترونية. إلى جانب مشاركة اللحظات المميزة عبر الصور والفيديوهات على منصات التواصل الاجتماعي، والاتصالات المرئية مع الأحباء والأصدقاء. كما يُتيح لنا إتمام المعاملات المالية عبر تطبيقات مثل تيكي أو التطبيقات المصرفية، وكذلك الوصول إلى الخدمات الحكومية أو استشارات الطبيب عبر الهوية الرقمية. حتى الأمور اليومية مثل الطباعة اللاسلكية وضبط أنظمة الإنذار والتدفئة وغيرها تتم بسهولة ويُسر عبر الإنترنت. هذا العالم الافتراضي يُضفي لمسات من السهولة والمتعة على حياتنا، ويجعل الأنشطة اليومية سلسة وممتعة للكثيرين.

ومع سعينا نحو السلامة الرقمية، يجب أن نؤكد على حماية كافة أجهزتنا وحساباتنا الرقمية. من الهواتف الذكية إلى الطابعات، وكل تطبيقاتنا الرقمية. فعلى غرار العالم الحقيقي، يتربص بنا المجرمون والمحتالون أيضًا في زوايا الإنترنت. هنا، سنقدم لك خمس نصائح أساسية لتعزيز أمانك وسلامتك أثناء تواجدك على الإنترنت. ستسهم هذه النصائح في تعقيد مهمة المجرمين الإلكترونيين وصعوبة التسلل والتلاعب بأمانك الرقمي.

1 - تأكَّد من وجود كلمات مرور آمنة لجميع أجهزتك وحساباتك. وذلك عن طريق اتّباع الخطوات التالية:

- قم باختيار كلمات مرور طويلة، فكلما طالت كلمة المرور كان ذلك أفضل. ويُفضل صياغة كلمات المرور باستخدام جمل كاملة.
- استخدم كلمة مرور مختلفة لكل حساب، واحفظ هذه الكلمات في مدير كلمات المرور.
- استخدم آلية التحقق الثنائي لتسجيل الدخول حيثما أمكن ذلك.

2 - لا تُهمل أبدًا تحديثات البرامج على أجهزتك الذكية فور توفُّرها

- الجهاز الذكي هو الذي يتصل بالإنترنت. مثل بعض الطابعات وكاميرات مراقبة الأطفال وأجراس الباب، وحتى المكنسة الكهربائية الروبوتية تعتبر جهازًا ذكيًا.
- من خلال تلك التحديثات، تكفل الشركات المصنِّعة دائمًا سلامة أجهزتك. لذا، لا تتجاهل هذه النوافذ المنبثقة!

3 - احرص على استخدام برامج مضادة للفيروسات

- هذه البرامج تقوم بفحص جهازك لاكتشاف جميع أنواع البرامج الضارة مثل الفيروسات، والبرمجيات الخبيثة، والتطبيقات الضارة.

4 - حافظ على إنشاء نُسَخ احتياطية بشكل منتظم

- في حالة اختراق جهازك، يمكن أن تخسر كل شيء. لذا، احرص على عمل نسخ احتياطية لملفاتك كإجراء احترازي.

5 - كن حذرًا وتحقق قبل النقر

- يُرسل المحتالون روابط مزيفة عبر البريد الإلكتروني أو الرسائل النصية أو طلبات الدفع. وذلك بهدف إقناعك بمشاركة بياناتك أو تحويل الأموال.

للمزيد من المعلومات حول وسائل السلامة الأساسية عبر الإنترنت، تفضل بزيارة
veiliginternetten.nl/5-tips-basisveiligheid