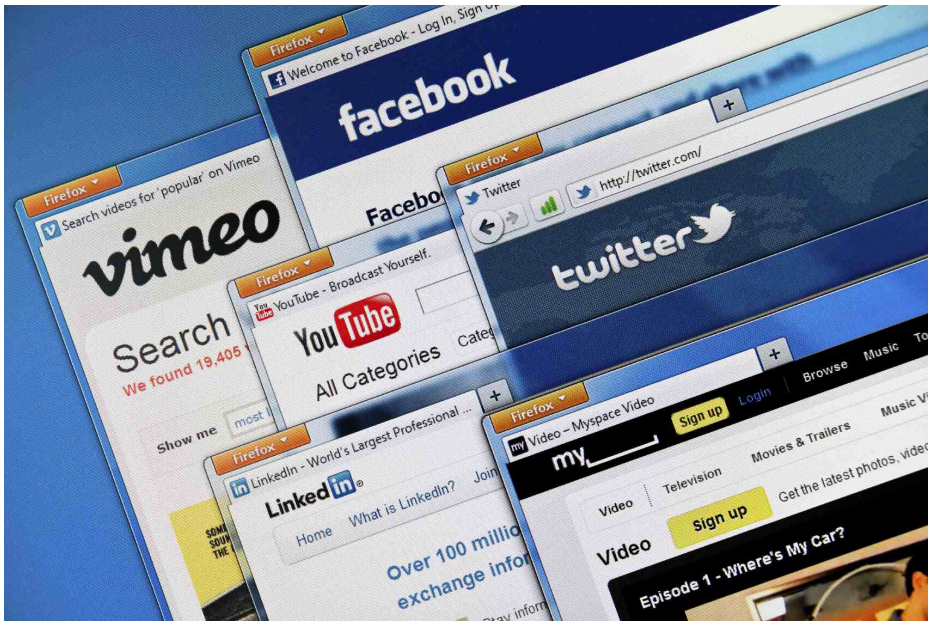
Six devoirs de cybersécurité pour la rentrée



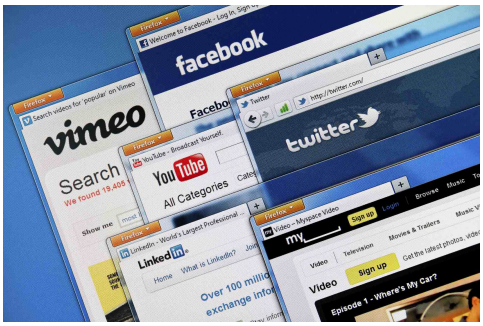
Six devoirs de cybersécurité pour la rentrée

La fin de l'été s'approche, ce qui implique le retour inévitable au travail. Après une période de repos est habituel que revenir à la routine ne soit pas facile, aussi quand il s'agit de mettre en pratique des mesures de sécurité et une précaution à nos dispositifs. Ces habitudes qui devraient déjà être acquises ne doivent pas s'abandonner et si elles n'existent toujours pas, c'est un bon moment pour commencer à se mettre à jour. La firme de sécurité Sophos Iberia propose ces conseils basiques pour une bonne routine de cybersécurité.

Des réseaux sociaux: publics ou privés ? À vous de choisir

Les réseaux sociaux ont déclenché un véritable phénomène international. Tout le monde s'y retrouve. Que l'on soit jeune ou plus vieux, tout le monde y est. Malgré le fait que ces soient des moyens intéressants pour se faire des amis, garder le contact, s'exprimer, partager ses émotions, ils présentent aussi une face cachée qui peut-être négative voire dangereuse car, parfois, **les réseaux sociaux peuvent donner une fausse sensation de sécurité.** Nous pensons que ce que nous publions peut seulement être vu par notre cercle plus proche d'amis, mais cela n'est pas toujours comme ça.

Il est nécessaire de configurer les **options de confidentialité** pour que les publications ne puissent pas être vues par n'importe quelle personne. Beaucoup d'utilisateurs ne comprennent pas cela et toute sa vie digitale est au découvert. Donc, comme première tâche, **accèdez aux options de confidentialité de vos réseaux sociaux (Facebook, Twitter, Instagram, et WhatsApp inclus) et décidez ce que vous voulez qu'il soit public**, et quoi est-ce que vous voulez maintenir dans le privé.



Sélectionnez bien vos contacts

Dans quelques réseaux sociaux, comme Twitter ou Linkedin, **il est habituel d'avoir beaucoup de contacts parmi lesquels nous ne connaissons pas tous personnellement.** Si nous maintenons un contrôle de ce que nous publions, il n'a pas de problème. Si nous sommes des utilisateurs qui partagent informations ou photographies plus personnelles, **nous devons être plus soigneux**: il est recommandable maintenir le profil privé (seulement à la vue des amis), et accepter comme contact seulement les personnes que nous connaissons. **Vous devez aussi penser à ce que vous partagez**, surtout quand il s'agit d'une information sensible comme la localisation.

Les mots de passe: différentes et privées

Il est très habituel entre les utilisateurs avoir un mot de passe unique pour quelques services. Avec la quantité de services que nous utilisons chaque jour, il est normal que nous ne puissions pas nous souvenir de toutes. **Mais il est recommandable avoir différents mots de passe dans chacun des comptes**, puisque **si quelqu'un réussit à accéder à l'une, il pourra accéder au reste.** Vous pouvez utiliser un gérant de mots de passe pour vous faciliter cette tâche.

Avant de déboucher, pensez deux fois

Les décharges, tant à travers des webs comme par courriers électroniques, sont la source de la plupart des infections des équipes, l'essor du ransomware est une bonne preuve de cela. C'est pourquoi, **il faut faire bien attention avant d'accéder à links**, des applications, des annonces ou webs qui peuvent être suspectes. Ah, et **cela ne s'applique pas seulement dans les Pcs aussi dans les smartphones.**

Fermez vos séances

Assurez-vous de fermer les séances de vos comptes quand vous aux dispositifs qui ne sont pas les vôtres, par exemple quand vous utiliserez un ordinateur public ou prêté. **Quelques services, comme Gmail ou Facebook, permettent de fermer les séances ouvertes de forme lointaine**, mais durant le temps qu'elles restent ouvertes et à la vue de n'importent qui **vos données sont exposés.**

Si vous le faites chez vous: pourquoi ne pas le faire en ligne?

Dans la porte de votre maison il y a une serrure: n'est pas? **Au réseau vous devez aussi mettre des empêchements pour que n'importe qui puisse accéder à vos informations**. Il est recommandable d'ajouter un mot de passe à votre ordinateur ou smartphone et aussi un code de déblocage. **Pour quelques utilisateurs il semble inconfortable, mais ces secondes extra peuvent vous éviter beaucoup de problèmes** comme que vos informations privées finissent aux mains étrangères.

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Six devoirs de cybersécurité pour la rentrée – Globb Security FR