Groupes 1 et 2 – COURS G105 et G204

L'INSECURITE SUR INTERNET

Naviguer sur Internet n'est pas sans risques ! Qu'il s'agisse d'intrusions visuelles directes chez soi par la Webcam intégrée à sa machine et opérable à distance, de contacts pris par le jeune public avec des loups déguisés en grand-mères, de piratages de cartes bancaires, d'abonnements onéreux malgré soi, de pseudo-interventions de dépannage à distance ou de cryptographie de ses données les plus sensibles, les occasions sont multiples d'être un jour ou l'autre victime des agissements des truands de la toile.
Il convient d'avoir conscience de tous ces risques et de prendre les mesures les plus adéquates, souvent de bon sens, pour s'en prémunir le plus possible.

1 – L'information disponible sur les risques les plus courants

Devant l'ampleur des phénomènes de piratage informatique, le gouvernement français a développé sur internet un site d'information que je recommande à chacun d'inscrire dans ses favoris de consultation : **www.cybermalveillance.gouv.fr**
La commission européenne a financé entre 2013 et 2015 un projet de lutte contre la cyber-criminalité (ACDC : Advanced Cyber Defense Center) dont les tenants et aboutissants sont consultables sur un site (en langue anglaise) : **www.botfree.eu**
Un certain nombre d'ouvrages traitent du sujet de manière sérieuse mais souvent assez technique et peu accessible au grand public. Notons tout de même un ouvrage accessible au plus grand nombre et plutôt bien conçu : « *Protéger son PC et faire face aux hackers* » de Remy Pelletier disponible en format e-book sur Amazon pour un prix modique.

2 – Quelques risques courants et leurs parades

L'intrusion par webcam commandée à distance : la webcam désormais systématiquement disponible sur les PC portables est un œil potentiellement ouvert sur votre activité (et sur votre présence/absence). Il convient donc d'obturer la webcam lorsque l'on ne s'en sert pas. Un post-it découpé au format de votre webcam devrait faire l'affaire.

L'abonnement « malgré soi » après période d'essai : vous acceptez, lors de la visite d'un site, une période d'essai d'un, deux ou trois mois en fournissant les indications relatives à votre carte bancaire. Après la période d'essai, vous vous retrouvez « abonné » sans en avoir pris conscience. Eviter absolument de délivrer les informations relatives à votre carte bancaire pour une procédure d'essai. Noter que la banque ne pourra jamais s'opposer au prélèvement et que la seule issue, en cas d'impossibilité de se désabonner, sera de faire invalider votre carte par votre établissement bancaire puis d'en rouvrir une nouvelle (ce qui n'est jamais gratuit!).

L'apparition d'une fenêtre déclarant que votre PC est infecté et qu'il convient d'appeler un numéro de téléphone pour se faire dépanner. Arnaque de plus en plus courante. Ne pas appeler ce numéro de téléphone (car il vous sera demandé de faciliter l'accès de votre PC à distance). Faire une photo de votre écran avec le numéro à appeler. Eteindre votre PC, lancer une analyse anti-virus complète et signaler immédiatement le numéro de téléphone sur le site : **www.internet-signalement.gouv.fr**

Le profilage à partir de vos requêtes et consultations de sites sur internet : la quasi-totalité des navigateurs et moteurs de recherche du marché historisent vos recherches et consultations de sites afin de déterminer vos goûts et centres d'intérêt. Vos « profils » ainsi déterminés et affinés au fil du temps sont ensuite vendus à des sociétés commerciales qui vous adressent « comme par hasard »

© 2017 - Pierre Monfort

les publicités relatives aux produits qui vous intéressent vraiment. Fuyez les navigateurs développés par les géants de l'internet et préférez les moteurs de recherche qui se déclarent en faveur de la protection de vos données personnelles (le navigateur **Firefox** allié au moteur de recherche **Qwant** semble être aujourd'hui une excellente alternative à ces procédures de fichage nocives et privatives de liberté). Dans tous les cas de figure, dans le paramétrage du navigateur, supprimer l'historisation des sites consultés, la suggestion de sites, le pistage de la navigation. Utilisez uniquement des fenêtres de consultation privées lorsque cela est possible.

Les attaques virales qui vont de l'espionnage de vos données et de vos comportements (spywares) à la déstabilisation du système d'exploitation Windows (modification du MBR : Master Boot Record ou altération de la FAT : File Allocation Table) et la menace la plus grave actuellement qui est le cryptage de vos données personnelles puis la remise de la clef de cryptage contre versement d'une rançon (le ransomware). Il n'existe pratiquement que cinq parades préventives :
- la **non-ouverture de mails et/ou pièces jointes** émanant de sources inconnues ou de copies de sites -souvent maladroites mais de plus en plus sophistiquées- comme le click sur des liens suggérés et non explicitement demandés. Passer outre à ces recommandations, c'est s'ouvrir sur un monde d'attaques virales diverses et jamais inoffensives.
- le **non-téléchargement de ressources culturelles protégées par droit d'auteurs** et dites « gratuites » sur des sites pirates qui contiennent systématiquement des virus et qui infecteront votre machine ou en prendront le contrôle sans que vous ne le sachiez
- l'**installation d'antivirus** (au moins Windows Defender, disponible en standard sous Windows), et un autre antivirus à votre choix en version gratuite ou payante en veillant à ce que les pare-feux disponibles soient activés (Kaspersky, Avast, McAfee, Norton,….). Lancer régulièrement une analyse complète de votre PC **après** avoir mis à jour le « moteur » de l'antivirus et sa « base de données virales » (généralement automatique sur les antivirus « payants » et à faire manuellement sur les antivirus « gratuits »)
- la **gestion attentive et régulière de sauvegardes de vos données** (préférez 2 supports différents toujours déconnectés hors procédure de sauvegarde : une clef USB et un disque dur externe par exemple. Travaillez toujours sur deux générations de sauvegarde au moins).
- la **mise à jours systématique de vos logiciels**, à commencer par le système Windows lui-même, un grand nombre de ces mises à jour consistant à « boucher » des failles de sécurité.

Les mauvaises rencontres sur la toile : attention aux contacts virtuels entre les ados et les loups déguisés en grand-mère. Activez le contrôle parental de vos fournisseurs d'accès internet, navigateurs et anti-virus ou mettez en œuvre des logiciels spécialisés. Créez sous Windows un compte limité en potentialités (pas d'accès administrateur) à réserver aux mineurs. Protégez votre compte d'administrateur par un mot de passe subtil et mixant chiffres, lettres majuscules et minuscules, signes. Ne le collez pas par post-it au dos de l'écran !

-=-=-=-=-=-

© 2017 - Pierre Monfort