Cybercriminalité et Réseaux Sociaux

Par Patrick LACORRE, Directeur de la Qualité et de la Sécurité de l'informatique de La Banque Postale et du réseau des bureaux de poste du Groupe La Poste.

Cette présentation se voulait pragmatique et la plus concrète possible. Pour ce faire, nous avons analysé 18 mises en situation de cas concrets d'utilisation d'internet et des réseaux sociaux que tout un chacun peut être amené à utiliser au quotidien.

Ainsi nous avons pu aborder :

- Le manque de confidentialité de la messagerie de part sa mondialisation et la facilité de piratage des mots de passe
- Le danger d'utiliser des services sur internet qui n'existent pas réellement (faux sites de Mandat Cash)
- L'usurpation de la bulle de confiance des comptes bancaires autorisés pour les transferts d'argent
- La recherche de «mules» pour permettre des opérations de blanchiment ou de financement terroristes par l'utilisation de la crédulité des personnes
- Les sollicitations frauduleuses par le stress pour récupérer des donnés confidentielles
- Les faux sites plus vrais que nature aux intentions malveillantes
- Les détournements de connexions sur des sites, soit grâce à des procédés techniques de prise de main à distance, soit par hameçonnage ou par dépôts de noms de domaines très proches des existants officiels et l'utilisation des fautes de frappe, etc.
- La surveillance sournoise des frappes sur le clavier ou des images dérobées correspondants à notre navigation et aux saisies réalisées
- L'approche et la manipulation par l'ingénierie économique et sociale
- Le risque d'usurpation d'identité suite à la transmission de pièces personnelles scannées
- Les automates de paiement trafiqués et les risques dus à la géo-localisation
- La prise en main de notre ordinateur avec les risques d'y introduire des éléments éligibles au pénal
- Les risques de chantage divers et variés (dossiers perdus, images pédopornographiques, etc.)
- La nécessité d'être toujours à jour dans sa protection virale
- La surveillance de l'utilisation de ses périphériques tels que les Webcam, son réseau interne domestique en Wifi, son imprimante
- Les dangers liés au fait d'exposer involontairement des informations sur les réseaux sociaux, etc.

Plus généralement nous avons enfin élargi le débat vers le domaine industriel, médical, domotique, avec tous les risques induits personnels et accidentels.
Cette présentation fut l'occasion également de parler du monde des «haktivistes» de tous types, politiques, idéologiques, frauduleux et de citer de nombreux exemples de mise en œuvre avec parfois des conséquences graves.

Il convient bien sûr de dédramatiser un peu le paysage, sachant que ce condensé de risques présentés ainsi, est le fruit de plusieurs années d'observation et cible souvent une population insuffisamment avertie et parfois négligente dans sa façon d'utiliser ces extraordinaires outils que sont internet et les réseaux sociaux par ailleurs.