

Les Banques organisent la riposte au cybercrime sur smartphone



Les banques songent à intégrer des logiciels dans leurs applications pour sécuriser les smartphones de leurs clients.

La pédagogie est la clef pour décourager les clients qui seraient tentés de télécharger des applications sur des « Stores Android » non officiels, de s'aventurer à débloquer leur smartphone ou encore de se connecter sur leur application bancaire depuis le réseau wi-fi d'un café, non sécurisé. « *La carte bancaire a beau être sécurisée, si le client divulgue son code, nos efforts de sécurisation sont vains. Il en va de même pour les usages sur le mobile, il y a des principes élémentaires de sécurité à respecter* », souligne Marc Zaroni, directeur sécurité des systèmes d'information du groupe BPCE.

Convaincre les clients

Comme pour la banque en ligne, les établissements veulent donc convaincre leurs clients de la nécessité de sécuriser leur smartphone. Certains les encouragent à télécharger des antivirus qui détectent les logiciels malveillants présents dans le téléphone et d'autres, comme Société Générale, promeuvent l'enregistrement du téléphone de leurs clients pour que la banque puisse vérifier, à chaque transaction, qu'il s'agit bien d'une demande officielle et non d'un pirate qui aurait capté des codes d'accès.

Ces outils restent optionnels car « *toute la difficulté est de garantir la sécurité sans dégrader l'expérience client. Nous ne voulons pas imposer de nouvelles pratiques brutalement* », explique un autre responsable Sécurité d'une grande banque française. Ce qui veut dire que « *les banques vont devoir agir à la place de leurs clients car ils n'auront pas la maturité nécessaire sur ces questions* », estime Clément Saad, fondateur de Pradeo, une jeune pousse spécialisée dans la cybersécurité...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *La riposte au cybercrime sur smartphone s'organise*,
Banque – Assurances