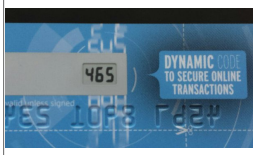
10 techniques de cybercriminels pour vous pirater votre carte bancaire | Denis JACOPINI

10 techniques de cybercriminels pour vous pirater votre carte bancaire

Pour sécuriser les achats par internet, Oberthur Technologies a imaginé une carte à puce avec CVV dynamique (Card Verification Value, les trois chiffres au dos de la carte). Un petit écran à affichage à encre électronique, comme les liseuses, est disposé au même emplacement que le CVV statique.



Une puce spécifique et une batterie insérées dans la carte permettent de gérer le changement de CVV toutes les heures, en totale indépendance par rapport à la puce de la carte. En parallèle, les banques émettrices pourront déléguer à Oberthur ou installer chez elles les serveurs fonctionnant avec le même algorithme et permettant ainsi de vérifier que la carte est bien en possession de son propriétaire au moment de l'achat sur internet. Un nouveau moyen de lutte contre la fraude.

Est-ce vraiment efficace ?
Revenons sur les principaux moyens de fraude à la carte bancaire.

1. VOL OU PERTE PHYSIQUE DE LA CARTE BANCAIRE
Exemple :
Vous faire voler votre carte bancaire ou l'égarer ne vous est jamais arrivé ? Vous êtes chanceux. Entre les professionnels de la chipe à l'affût de la moindre inattention et les étourdis comme moi qui ont beaucoup de mal à rester concentré sur ce qu'ils font s'ils ont trop de sollicitations à traiter en même temps, il est tout de même courant qu'on ne retrouve plus sa si précieuse CB. Horreur ! Danger ! Fin du monde ! se dit-on si ça nous arrive.
Le risque :
Il est clair que le nouveau propriétaire d'une carte bancaire perdue ou volée n'a que très peu de temps pour agir. Il pourra rapidement faire des achats sur Internet avec cette bourse malhonnête, ou pourra également revendre cette carte ultra-fraîche sur le DarkNet pour un usage frauduleux similaire.
Pour se protéger :
Par anticipation, vous pourrez gratter le cryptogramme
Si c'est trop tard
Appelez le 0 892 705 705, le serveur interbancaire pour la mise en opposition des Cartes Bancaires.

2°/ COPIE AU DISTRIBUTEUR SOL. : CONFIANCE A PERSONNE DISCRET
Exemple :
Vous allez retirer de l'argent dans un distributeur (isolé la plupart du temps) et faites attention aux regards indiscrets et aux personnages inquiétants pouvant roder autour. Le danger peut venir de là où on ne l'attend pas. En effet, les pirates professionnels peuvent maquiller le distributeur de votre banque avec un appareil enregistrant la bande magnétique de votre carte au moment ou vous l'introduisez (skimmer) et enregistrant le code de votre carte soit par le clavier (piégé) ou par une discrète caméra captant votre code en le filmant par dessus le clavier.
Le risque :
Le pirate agissant ainsi pourra, à partir de la lecture de la bande magnétique reproduire votre carte bancaire et avec le code qu'il vous a discrètement dérobé, reproduire un clone de votre carte. Les informations captées étant numériques, elle peuvent être vendues ou envoyées dans le monde entier.
Pour se protéger :
Prenez l'habitude d'aller dans un distributeur de billets connu.
Si c'est trop tard
Appelez le 0 892 705 705, le serveur interbancaire pour la mise en opposition des Cartes Bancaires.

3°/ VOL CHEZ LES COMMERCANTS
Exemple :
Il a été démantelé à plusieurs reprises en France des réseaux de cybercriminels embauchant dans des bars ou des cafés des serveurs équipés d'appareils portables permettant la copie de la bande magnétique de la carte bancaire. Puisqu'ils ont la CB dans la main, ils peuvent également recopier le cryptogramme et discrètement vous voir taper votre code.
Le risque :
Il est clair que le nouveau propriétaire d'une carte bancaire dont la piste magnétique a été volée sans que le vrai propriétaire le sache, a tout son temps pour agir. Les informations captées étant numériques, elle peuvent être vendues ou envoyées dans le monde entier.
Pour se protéger :
Ne vous séparez jamais de votre carte sauf pour payer et lorsque vous les avez sous les yeux (la carte et le serveur).
Si c'est trop tard
Appelez le 0 892 705 705, le serveur interbancaire pour la mise en opposition des Cartes Bancaires.

4°/ VOL DES COORDONNÉES PAR NFC
Exemple :
La technique de vol de vos coordonnées bancaires par NFC consiste à utiliser un lecteur de cartes NFC portable, à distance et autonome et à se balader dans des lieux ou la densité de passants est très forte (par exemple dans le métro). L'appareil autonome pouvant aisément être camouflé dans un sac à dos détectera les CB se trouvant dans son rayon de détection, enregistrera les données émises par les CB répondant aux commandes NFC envoyées par l'outil du pirate.
Le risque :
Il est clair que le nouveau propriétaire d'une carte bancaire dont la piste magnétique a été volée sans que le vrai propriétaire le sache, a tout son temps pour agir. Les informations captées étant numériques, elle peuvent être vendues ou envoyées dans le monde entier.
Pour se protéger :
Protégez votre carte bancaire dans une boite ou un coffret metallique (la pochette de protection des boitiers Telepeage peut aussi bien faire l'affaire).
Si c'est trop tard
Appelez le 0 892 705 705, le serveur interbancaire pour la mise en opposition des Cartes Bancaires.

5°/ OUVERTURE D'UN COMPTE EN USURPANT L'IDENTITÉ D'UNE VICTIME
Témoignage
"Au début du mois de septembre, ma colocataire m'a avertie que quelqu'un d'[une banque] voulait me joindre. Comme le numéro que la personne avait laissé était avec un indicatif régional que je ne connaissais pas, j'ai cru qu'on voulait me vendre des produits financiers et j'ai failli ne pas rappeler comme je partais en vacances le lendemain. Finalement, j'ai appelé et le numéro m'amenait directement au département des fraudes. On m'a demandé si j'avais un compte avec [la banque en question] (non), et on m'a dit qu'on suspectait que j'ai été victime d'un vol d'identité. Une personne avait commandé une carte de crédit en ligne en mars, en changeant mon numéro d'appartement et avait fait des transactions pour près de 14 000 $, somme bien sûr qu'elle n'avait jamais remboursée. On m'a suggéré d'aller au poste de police porter plainte et de passer en succursale si je voulais plus d'informations, choses que j'ai faites."
La Technique
Le fraudeur possédait nos noms, adresses exactes et numéros d'assurance sociale. Il commandait des cartes de crédit en ligne et indiquait les bons noms et les bonnes adresses, à une différence près : il n'indiquait pas le bon numéro d'appartement. De ce fait, nos voisins qui recevaient des lettres qui ne leur étaient pas adressées (mais qui comportaient les cartes de crédit) les laissaient sur les boites postales et le fraudeur les ramassait, tout simplement.
Le moyen de se protéger
Lorsque ça arrive, il faut que les gens ne déposent pas des lettres qui ne leur sont pas adressées sur le dessus de leur boîte, mais aillent plutôt les porter directement aux personnes dont les noms apparaissent sur l'enveloppe ou au pire, les remettent dans des boîtes aux lettres de la Poste en indiquant mauvaise adresse.

6°/ INFECTION DES DAB (2003-2015)
Exemple :
Comme les ordinaeurs, smarphones et tablettes, les distributeurs automatiques de billets ont leur Virus. Dernièrement, en 2015, GreenDispenser, puisque c'est ainsi qu'il est baptisé, vient s'ajouter aux redoutables Suceful, Plotus ou Padpin pour le malheur des banques et de leurs clients. Le virus est introduit dans le D.A.B. (distributeurs automatiques de billets) et va en perturber le fonctionnement au point ou ce dernier distribuera des billets à la demande, sans suivre les procédures pourtant savamment verrouillées.
La Technique
Le fraudeur en fonction du type de DAB vient utiliser une de ses failles pour pouvoir lui faire croire qu'une carte a été rentrée et que de l'argent a demandé d'être retirée sans limite (sauf le stock).
Le moyen de se protéger
C'est aux constructeurs de DAB de mettre à jour et protéger leurs appareils.
SUCEFUL : LE MALWARE NOUVELLE GENERATION

7°/ VOL DES COORDONNEES PAR PHISHING
Exemple :
Chaque seconde, sont envoyés dans le monde un peu plus de 2,5 millions d'e-mails. Cela représente un peu plus de 210 milliards d'e-mails par jour (en moyenne 64 e-mails par jour et par personne). Un peu plus de 56 % représente du SPAM. Cela fait un peu plus de 36 spams par jour et par personne. 11% de ce spam est du Phishing. Cela fait aux alentours de 4 e-mail de phishing (hameçonnage) par jour et par personne, dont le seul but de ces e-mails est de vous récupérer identifiants mots de passe et coordonnées bancaires.
Selon le site Internet "jegardecapourmoi.com", 71 % des attaques d'hameçonnage utilisent le nom et le logo des institutions financières.
La Technique
Se faire passer pour un organisme (financier de préférence) de confiance, prétexter une quelconque bonne raison pour gentiment demander (le plus souvent pour vérification) à la victime de vous communiquer les informations de sa carte bancaire pour pouvoir ensuite les vendre sur le DarkNet ou les utiliser.
Le moyen de se protéger
Apprenez à détecter les e-mails de hameçonnage, de harponnage ou de phishing.

8°/ VOL LORS D'UN ACHAT SUR INTERNET (CLIENT/SERVEUR)
Exemple :
Soit l'ordinateur de la victime est infecté (par un Virus "Man In the Browser")
Soit la ligne internet est piratée ("Man in the Middle")
Soit le serveur peut avoir une faille (exemple de "Heart Bleed")
La Technique
Utiliser une faille de l'équipement informatique du client ou du commerçant pour récupérer les données bancaires,
Le moyen de se protéger
Mettre un logiciel de sécurité à jour

9°/ PIRATAGE DES BASES DE DONNÉES (INJECTION SQL)
Exemple :
Target s'est fait voler 70 millions de données personnelles de ses clients dont 40 millions de coordonnées bancaires.
La Technique
Utiliser une faille des serveurs pour accéder à leur base de données. Les données non protégées peuvent alors être bavardes et riches en informations confidentielles et sensibles tel que des coordonnées bancaires.
Le moyen de se protéger
N'utilisez que des cartes bancaires virtuelles et à usage unique.
N'enregistre jamais vos CB par facilité dans les sites Internet

10°/ PIRATAGE DES ORDINATEURS
Exemple :
Parce qu'il est tellement plus facile de noter les coordonnées de sa carte bancaire dans un fichier dans un ordinateur plutôt que d'essayer de s'en rappeler, ces informations ultra sensibles, si elle ne bénéficient pas d'un soin particulier, ne résisteront pas à la curiosité professionnelle de pirates informatiques.
La Technique
Scruter les disques durs à la recherche de tout ce qui pourrait ressembler à 16 chiffres.
Le moyen de se protéger
Utilisez un cryptage fort pour sécurités des informations bancaires et sensibles

LA BIOMETRIE AU SECOURS DE LA FRAUDE PAR CARTE BANCAIRE
La Banque Postale se lance dans la biométrie vocale car, en ce début de mois de mars 2016, elle vient d'obtenir l'autorisation de la CNIL (Commission nationale de l'informatique et des libertés) d'utiliser cette technologie de reconnaissance vocale pour sécuriser les paiements en ligne de ses clients. C'est une première en France.
Pour effectuer un paiement sur Internet, le client recevra un appel de la banque pour s'identifier. Il lui suffira alors de prononcer quelques mots pour vérifier son identité. Ensuite il pourra payer.

INFOS DIVERSES
2012 :
500 milliards d'euros de transactions en France;
450 millions d'euros de fraudes (0,08%).
Avant de faire des achats importants, les pirates font de petits dons à des œuvres charitables. Une manière philanthropique de tester la carte. Ensuite, celle-ci servira à toutes sortes de trafics, mondialisés ou locaux.
Les grands commerçants s'équipent désormais de la protection 3D Secure – sans quoi ils subissent le coût de la fraude –, et travaillent à l'obtention du standard de sécurité PCI DSS. Pour obtenir cette certification, l'entreprise subit un check-up complexe (900 points sont contrôlés), mais fondé sur une philosophie simple : tout doit être mis en œuvre pour protéger les données des Cartes bleues des clients.

Une fraude qui a marqué l'actu :
Fin 2008, le président Sarkozy s'était aperçu que de petits montants avaient été prélevés sur son compte pour un total de 170 euros.

*Enfin, pour répondre à la question "**La protection par cryptogramme dynamique, est-ce vraiment efficace ?**", je répondrais : "Ca dépend".*
Oui dans presque tous les cas pour lesquels le numéro de CB a été dérobé, mais vu que de nombreux pays ne demandent pas le cryptogramme et que certains sites Internet le demandent mais ne le vérifient pas, le consommateur peut se sentir protégé pour des achats qu'il effectue en France et en Europe, mais pas pour des achats effectués ailleurs sauf s'il s'est renseigné sur le respect des normes de sécurité 3DS par la banque du commerçant .

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

- Conférences, tables rondes, rencontres autour des thèmes de la cybercriminalité et de la protection des données personnelles;
- Formateur et chargé de cours en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
- Consultant en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
- Expertises et avis techniques en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;

Contactez-nous

Réagissez à cet article

Sources :

http://www.agefi.fr/banque-assurance/actualites/hebdo/20160210/oberthur-technologies-lance-carte-a-cvv-dynamique-155903

http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html

https://www.jegardecapourmoi.com

http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html

http://www.bienpublic.com/actualite/2013/10/10/dijon

http://www.lanouvelletribune.info/societe/vie-societale/technologie/25616-greendispenser-un-nouveau-virus-voleur-de-billets-de-banque

https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015