Mémento du petit-déjeuner conférence organisé jeudi 17 mai de 8h30 à 10h - Provadys Nantes

Par Julien SOUDÉE, Project Expert Information Security

Les paiements bancaires sur Internet : les bons réflexes à avoir pour payer sans risques.

Bien que le paiement par Internet soit une tendance à la hausse, les principes de sécurité ne sont pas toujours maîtrisés par les clients ou par les cybercommerçants.
Avoir les bons réflexes de sécurité sur Internet permet d'éviter le vol des données bancaires des utilisateurs et de préserver la confiance dans le système.

Pour procéder à des paiements en toute confiance sur Internet, voici nos conseils sur les précautions à prendre pour une utilisation sécurisée.

a. Choisir les sites marchands pour effectuer ses achats :

Il est primordial de sélectionner des sites de confiance, dont la réputation et la fiabilité sont largement reconnues.
Dans tous les cas, il est indispensable que le site propose un niveau de sécurité à jour : HTTPS s'appuyant sur le protocole TLS 1.1 minimum (et 1.2 idéalement).

Figure 1 - Exemples de sites sécurisés

Votre navigateur peut aussi vous aider à détecter les sites trop peu, voire non sécurisés (à condition qu'il soit lui-même à jour !).

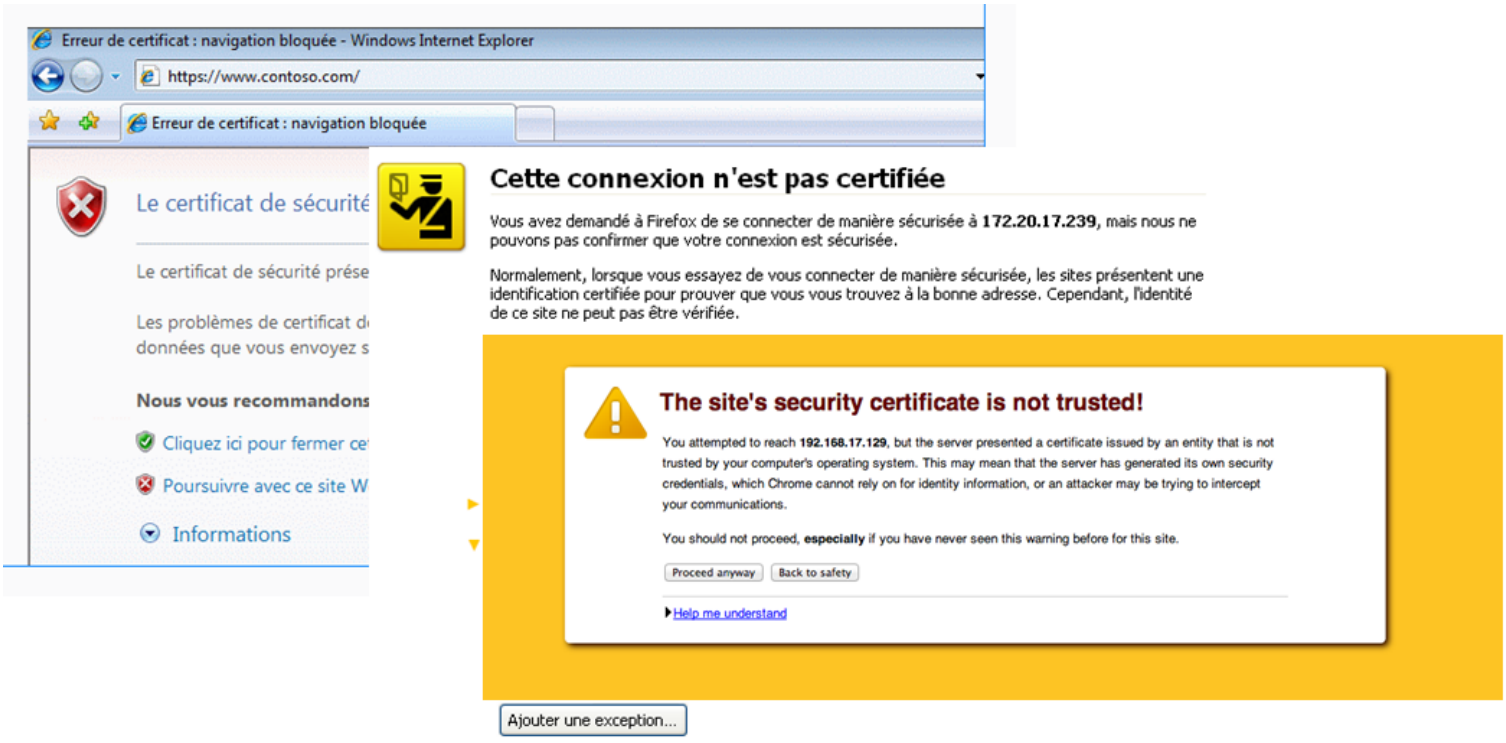

Figure 2 - Exemples de messages d'alerte des principaux navigateurs Internet

b. Éviter les réseaux publics pour effectuer ses achats :

Il est fortement déconseillé de réaliser des achats ou toute autre opération sensible (comme se connecter à sa banque en ligne) sur des ordinateurs « publics », ou via des réseaux Wi-Fi publics.

En effet, les ordinateurs des cyber-cafés sont souvent mal sécurisés (il y a beaucoup de passage, les URL visitées ne sont pas toujours sûres, de nombreuses clés USB sont branchées et il est impossible de savoir pour quel dessein elles ont été utilisées…).
De même, les réseaux Wi-Fi publics sont régulièrement usurpés (ce que l'on appelle un rogue AP).
Si vous avez besoin de vous connecter en mobilité (paiements bancaires ou connexion à sa banque…), privilégiez la connexion 4G de votre téléphone.

c. Limiter les risques de vol en sécurisant ses données CB :

Voici un échantillon de moyens permettant de limiter les risques de vol de vos données CB.
Les deux principales solutions sont l'utilisation de Cartes Virtuelles Dynamiques (CVD ou e-card) et les Staged Wallets (type Paypal) :
- Les CVD sont des cartes générées lors de l'achat qui permettent d'utiliser un numéro valable une seule fois, différent du numéro réel de votre carte bancaire. Ce service est généralement proposé par votre banque.
- Les Staged Wallets sont des portefeuilles électroniques sur lesquels vous chargez de l'argent et que vous utilisez ensuite comme vous le souhaitez (là où ils sont acceptés).
Dans ces deux situations, vous sécurisez les données de votre carte bancaire.
Dans les deux cas, le point sensible en termes de sécurité est déplacé au niveau de l'authentification au service : service de génération du numéro de carte virtuelle, ou accès au compte du portefeuille électronique. Choisissez des mots de passe forts et uniques.

Il y a quelques années (en 2015), les premières cartes avec CVV dynamiques ont également vu le jour, permettant de limiter le risque d'usurpation, car les trois chiffres aux dos de la carte changent régulièrement (toutes les N secondes ou minutes, au choix de la banque).

En respectant ces préconisations, vous préserverez la sécurité de vos données bancaires sur Internet. Cependant, les cybermenaces étant en constante évolution, il est indispensable de maintenir une vigilance accrue. Au moindre doute, passez votre chemin.

À propos :
Provadys est une société de conseil, d'audit et de formation, spécialiste des technologies de l'information, et qualifiée PASSI RGS par l'ANSSI pour ses prestations d'audit et de tests d'intrusion.
Provadys est certifiée en tant que « QSA Company », ce qui lui permet de réaliser les audits de certification PCI DSS.
Les consultants de Provadys, experts en Cybersécurité, vous apportent également leurs retours d'expérience pour vous accompagner dans vos projets de mise en conformité, que ce soit sur PCI DSS ou sur d'autres référentiels de sécurité (ISO 27001, ARJEL, LPM, GDPR, ISAE …).

Nous contacter :
contact-ouest@provadys.com
Tél : 02 55 59 01 10