

*Lien : [Vidéo : vers la refonte des cartes d'identité, bientôt dotées d'un nouveau format et d'une puce - ZDNet](#)*

Date : **Le mercredi 11 déc. 2019 à 12:41**

Auteur : Par Pierre Benhamou

**Technologie** : *Le gouvernement planche actuellement sur une refonte des cartes d'identités. Biométriques, ces dernières seront dotées d'un nouveau format de type cartes de crédit ainsi que d'une puce.*

- *Type carte crédit sans contact*
- *Cette nouvelle carte d'identité "devra également inclure une photographie et deux empreintes digitales du titulaire de la carte, stockées à un format numérique, sur une puce sans contact.*
- *Publier le 2 août 2021 selon européen*

*Lien : [Les iPhone peuvent servir de clé de sécurité physique pour les comptes Google - ZDNet](#)*

Date : **Le jeudi 16 Janvier 2020**

Auteur : L'agence EP

**Technologie** : *Toute personne possédant un iPhone peut l'utiliser comme clé de sécurité pour une authentification à deux facteurs lors de la connexion à un compte Google.*

- *Deux authentification sur SMART Lock pour iOS pour mettre la sécurité de Google*
- *Le système peut fonctionner via une connexion Bluetooth sur Chrome OS, iOS, macOS ainsi que des ordinateurs Windows 10 avec Google Chrome*
- *La principale différence avec la version Android est que dans celle-ci, la clé de sécurité est intégrée aux terminaux.*
- *Sécurisé le compte pour éviter les attaques et perde téléphone le journaliste, activistes, chefs d'entreprise, équipes de campagnes électorales, i faut d'enregistrer une clé de sécurité de sauvegarde pour votre compte et de la conserver dans un endroit sûr.*

Lien : [Ce malware use d'une tactique imparable pour se répandre - ZDNet](#)

Date : **Le lundi 24 mai 2021 à 17:48**

Auteur : Danny Palmer

**Sécurité** : *Le malware STRRAT, basé sur Java, crée une porte dérobée dans les ordinateurs infectés, mais distrait les victimes en agissant comme un rançongiciel. Une tactique insolite mais payante.*

Inconvénient :

- Phishing met en place un virus de trojan à distance sur un ordinateur et créer une web shell pour aller dans les ordinateurs des personnes afin voler les information : es noms d'utilisateur, les mots de passe et autres données personnelles des victimes
- Le malware ajoute une extension de nom de fichier .crimson aux fichiers afin de faire passer l'attaque pour un **ransomware** sans crypte
- Envoie des messages email accompagnés d'une image se présentant comme une pièce jointe qui semble contenir des informations sur le transfert supposé et comme en cliquez cette image ou lien et il peut contrôler tous dans notre ordinateur

Avantage :

- Il faut se méfier des messages inattendus ou inhabituels
- faire preuve de prudence lorsqu'il s'agit d'ouvrir des courriels et des pièces jointes provenant d'adresses électroniques étranges ou inconnues
- Installe antivirus pour empêcher les courriels malveillants venir dans le boîte email ainsi le risque ouvre le lien de message sois éliminer

Lien : [Comment et pourquoi sécuriser son poste de travail ? - ZDNet](#)

Date : **Le jeudi 01 avril 2021 à 08:00**

Auteur : APM

**Technologie** : *Les changements d'habitudes de travail des salariés n'ont pas échappé aux pirates, dont les attaques redoublent. Le développement du travail à distance oblige les entreprises à repenser leur sécurité et aussi à sensibiliser aux menaces.*

Il y a plusieurs entreprise à été menacer en 2020. C'est pour sa en met en place les différentes sécurités

Le sécurité sont :

- Ne mélangez pas usages personnel et professionnel sur le même ordinateur
- Installez les mises à jour de sécurité sur vos terminaux
- Installez et activez un antivirus
- Sécurisez vos comptes
- Sauvegardez vos données
- A tenir au courant de menace à votre équipe