Pistez les pirates avec Gmail

Le piratage des comptes e-mails est l'un des **sports favoris des pirates en herbe** et autres hackers (pour ne pas faire de jaloux). Et pour cause, les courriels contiennent souvent énormément d'informations personnelles exploitables pour mener d'autres opérations malveillantes, à commencer par l'usurpation d'identité. Ce fut d'ailleurs la méthode employée par Hacker-croll pour pénétrer l'administration du réseau de Twitter.

Mais comment savoir que son compte de messagerie a été piraté? Google y répond partiellement en implémentant **un outil de détection géographique**. Le principe est simple : Google a les moyens (comme tous les fournisseurs de services en ligne) d'analyser l'adresse IP de la connexion à un compte web afin de la situer géographiquement dans le monde. Si le système constate une différence notable de lieu de connexion entre deux utilisation de Gmail espacées de quelques heures, l'application émet une alerte indiquant le pays d'origine de la dernière connexion.

Il est évident que si vous consultez Gmail de France et que le webmail vous alerte d'une récente connexion effectuée depuis la Chine (simple exemple), vous serez en mesure d'estimer qu'il y a quelque chose qui cloche là-dedans. Plus sérieusement, l'outil d'alerte de Gmail va même jusqu'à indiquer l'origine géographique des dernières connexions web. Une analyse de la navigation (fixe, mobile) ou des consultations de comptes POP est également affichée, histoire de confirmer (ou infirmer) les doutes éventuels. L'interface propose alors de **changer le mot de passe** histoire de barrer la route au pirate.

Malgré le progrès affiché (que les dissidents chinois ne seront pas les seuls à apprécier le service) le système n'est cependant pas exempts de défaut. Pour des raisons probables de **respect de la vie privée**, Google se contente de comparer l'origine géographique des connexions uniquement à l'échelle internationale. Un compte piraté dans le même pays que celui de son utilisateur légitime ne sera vraisemblablement pas signalé. D'autre part, si le pirate décide de changer le mot de passe du compte usurpé, ce dernier restera inaccessible à son propriétaire initial qui, pour le coup, constatera immédiatement son piratage.

Proposée sur les comptes Gmail individuels, cette surcouche de sécurité sera prochainement implémentée à **Google Apps** proposé aux organisations professionnelles et au monde de l'éducation notamment.

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity.
Learn more

This account is open in 4 other locations.
(Location may refer to a different session on the same computer.)

Concurrent session information:

Access Type [?] (Browser, mobile, etc.)	**Location (IP address) [?]**
Browser	United States (CA) (172.18.222.92)
Browser	United States (CA) (172.18.112.221)
Browser	United States (CA) (172.18.28.15)
Browser	United States (CA) (172.18.28.14)

Sign out all other sessions

Recent activity:

If the activity below doesn't look like yours, change your password immediately Learn more

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Unknown	Poland (83.17.123.186)	Mar 8 (2 days ago)
Browser	* United States (CA) (172.18.113.120)	1:03 pm (0 minutes ago)
Google Toolbar	* United States (CA) (172.18.113.120)	1:03 pm (0 minutes ago)
Browser	United States (CA) (172.18.112.221)	1:03 pm (0 minutes ago)
Browser	United States (CA) (172.18.113.120)	1:02 pm (1 minute ago)
Google Toolbar	United States (CA) (172.18.113.120)	1:02 pm (1 minute ago)

Alert preference: Show an alert for unusual activity. change

* indicates activity from the current session.

This computer is using IP address 172.18.113.120. (United States (CA))