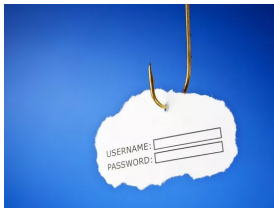




Hijackers get up close and personal with hacked accounts

Elizabeth Weise, USATODAY Published 10:08 a.m. ET Nov. 6, 2014 | Updated 10:13 a.m. ET Nov. 6, 2014



(Photo: Shutterstock)

SAN FRANCISCO - Getting your email account hijacked is creepier than you know, a study by Google scientists finds.

In the vast majority of compromised email accounts, the process is automated, facilitated by so-called spambots that use the hacked account to spew spam.

But in a first-of-its-kind study, the Google researchers observed what they call manual account hijacking.

In these attacks, the attention is very personal.

There are no mindless programs running on distant servers. Instead, the hijacking is handcrafted, performed by offices full of low-level workers who clock in for a regular business day.

Most of the hijackers appear to be working out of China, Ivory Coast, Malaysia, Nigeria and South Africa, the researchers found.

"One benefit of account hijackers specializing by language is that they can focus on a smaller market. For instance, French-speaking groups usually just target France, whereas English-language groups are going after more than half the world," said Borbala Benko. Based in Zurich, she is the engineering lead on Google's anti-hijacking work.

The hijackers are very disciplined and regimented. They get an hour off for lunch and don't work weekends.

What they do do is "read your emails. They spend time in your account. They go through your trash. There's a sense of violation to it," said Elie Bursztein, who leads the anti-abuse team at Google's Mountain View, Calif. headquarters.

He is the lead author on a paper documenting their findings that is being presented Thursday at the [Internet Measurement Conference](http://conferences2.sigcomm.org/imc/2014/) (<http://conferences2.sigcomm.org/imc/2014/>) in Vancouver, British Columbia.

This type of manual account hijacking is rare. The team examined system logs Google collected between 2011 and 2014. They found just nine incidents per million Google users per day.

But in these cases, the hijackers spent a significant amount of time in individual accounts.

To gain access, they overwhelmingly use phishing—68% of successful hijacks were linked to phishing sites or emails.

[Don't become a victim of spear phishing](https://www.usatoday.com/story/money/personalfinance/2014/10/18/malware-data-breach-phishing/17458411/)

(<https://www.usatoday.com/story/money/personalfinance/2014/10/18/malware-data-breach-phishing/17458411/>)

Phishing involves the use of fake websites or emails or websites to lure the unsuspecting to input their login ID and password.

In the emails, a common story is "I've been mugged in Manila and they stole everything—I need you to wire me money."

Phishing websites often mimic banking or other official sites. Sometimes they tell users to update their credentials or their email account will be deactivated.

How successful the phishing pages or emails are depends on how believable they are. Some had success rates as high as 45%, while poorly done ones were as low as 3%, the researchers found.

Once the user typed account information into the phishing site, the hijackers pounced very quickly.

Using decoy email accounts, the Google researchers found that in 20% of cases the hijackers were into the account within 30 minutes. Half of the accounts were accessed within seven hours.

In most cases, the first thing the hijackers did was lock the victim out of their own account, so they couldn't warn anyone.

The hijackers typically spend three minutes rifling through the inbox, sent mail and trash of an account to see if there's anything worth stealing, such as banking information.


Next the miscreants use the information they find in the account to craft customized phishing messages or more scam emails, which go out to the victim's contact list.

Google researches these types of attacks to better bullet proof its customers from such hijacks, Bursztein said.

The best way to avoid them is to use two-factor authentication and keep contact information updated so you can immediately be notified if it appears your account has been compromised.

"If you just put a better lock on your accounts, you can keep them out," said Bursztein.

Read or Share this story: <http://usat.ly/1qrtC4m>



See how SMS-Magic helps your business engage customers with conversational texts. Ready for your next challenge.

WATCH DEMO

salesforce appexchange

The advertisement is a horizontal banner with a blue-to-green gradient background. On the left, there is a white button with the text "WATCH DEMO". To the right of the button, there is a white square containing an orange double-headed arrow icon. Further right, a cartoon cat with glasses is sitting in a red boat on a body of water. In the background, there are green trees and a blue sky. On the far right, there are logos for "salesforce" and "appexchange".