This is how your Gmail account got hacked

by Jose Pagliery  @Jose_Pagliery

December 29, 2014: 1:37 PM ET

How easy is it to steal your passwords?

If your Gmail account got hacked, blame your friends.

You are 36 times more likely to get scammed if your contacts' accounts have been hacked, according to a study released this week by Google (GOOG).

It's rare. On an average day, only nine in 1 million accounts get stolen. But when it happens, the operation is swift. These are professional criminals at work, looking through your email to steal your bank account information.

The criminals are concentrated in five countries. Most of them live in China, Ivory Coast, Malaysia, Nigeria and South Africa. But they attack people worldwide, duping them into handing over Gmail usernames and passwords.

Google has effective scans to block them and emergency options to get your account back. But criminals still manage to pull off the attacks.

Here's some more of what Google found in its three-year study.
Effective scams work 45% of the time. This number sounds huge, but well-crafted scams can be convincing. They send official-looking emails requesting your login credentials. And sometimes they redirect you to a page that looks like a Google login, but it's not.

Safety tip: Don’t ever email your username or password -- anywhere. And always check the Internet address in the URL above to ensure you’re at the actual Gmail site.

They usually steal your account in less than a day. Once they have your login credentials, the average criminal hijacks your account within seven hours. For an unlucky 20%, the bad guys do it in just 30 minutes. Then they change your password to lock you out.

Safety tip: Sign up for account alerts on your phone or a backup email. And move fast.

Related: Apps aimed at children collect a shocking amount of data

It takes only 3 minutes to scan your email for valuable stuff. They're looking for any email that shows your bank account information and images of your real life signature. They also search for login credentials for other accounts at Amazon (AMZN) or PayPal. They use the email search feature, looking for phrases like "wire transfer," "bank" and "account statement."

Safety tip: Perform this search yourself. Go ahead and erase any email with this sensitive data. Don’t leave this stuff lying around.

Expect your friends to get preyed on too. Criminals will send emails in your name asking friends for money. Typically, they use a sob story, claiming you got stuck somewhere and need help.

Fraudsters are smart at keeping this under the radar too: 15% of them create automatic email rules that forward your friends’ responses to another email address. So even if you get your account back, you won’t know your friends were targeted, because you’ll never get their responses.

Worst of all? Sometimes fraudsters delete all your emails and contacts to prevent you from warning friends afterward. Google has an account recovery option to bring them all back -- but that’s only if you actually recover your account.
Safety tip: Just make it impossible to break into your email in the first place. Sign up for two-step authentication, a second password you get by text message. It’s an extra 30 seconds on every new computer, but it’s worth it in the long run.

CNNMoney (New York)
First published November 7, 2014: 8:24 AM ET