

All 2011

Give a Gift, Save 57%

The CHRISTIAN SCIENCE
MONITOR

Automate your lead scoring
and nurturing with 

DOWNLOAD
THE FREE WHITE PAPER

AdChoices
About these ads

Anthony Weiner Twitter hack? What he should have done.

Amid the furor around an indecent photograph sent from Congressman Weiner's Twitter account, the question arises: What should you do once an account has been hacked?

By Gloria Goodale, Staff writer / June 2, 2011



Rep. Anthony Weiner (D) of New York, waits for an elevator near his office on Capitol Hill in Washington, on Thursday, June 2. The Congressman has said that a hacked Twitter account led to the release of an indecent photograph, but says he has hired private investigators to determine what happened.

Susan Walsh/AP

Enlarge

The line "I got hacked" has become the latest political fig leaf for social media mistakes.



In Pictures: Who is Rep. Anthony Weiner?

Related stories



How attack on Google's Gmail skirted US security roadblocks

Twitter scandal: a mess for Anthony Weiner, a lesson for Congress

How 'cookiejacking' could steal people's Facebook passwords

Topics

Internet • Science and Technology • Technology • Social Software and Tagging • Government and Politics • Politics

It has emerged again, trotted out by New York Democratic Congressman Anthony Weiner after a suggestive photo was sent from his personal Twitter account.

Hacking happens often enough that there should be a well-known, universal response – but so far, one has not emerged. And in this helter-skelter approach to security, untold volumes of information remain vulnerable, notes security expert David Koretz. "There has been a rush to move everything online," from political communications to private finance, he says. Without an equal push for security in the digital sphere, he says, "we are at risk – not just in the way we communicate, but in everything we do online."

RECOMMENDED: Five simple ways to protect yourself from identity theft

So what should you do if you think your account has been hacked?

"If [Representative Weiner] really was hacked, that would fall under federal cyber crimes or wire-tapping laws, and it would be intra-state," says Mr. Koretz, CEO of Mykonos Software, a vendor that secures websites and applications. "Your next stop

would be the FBI, if you believe it's domestic."

Of course, it always helps to be a national figure. Politicians have more resources when it comes to digital transgressions, notes Patrick Kerley, senior digital strategist at Levick Strategic Communications. "A congressman has more access than an average person, and would reasonably be expected to take immediate steps – whether it's the FBI or the Capitol Police."

"If someone stole the letterhead of a public figure, that would be fraud," notes David Mercer, a former deputy finance director of the Democratic National Committee. Sending a digital message under their name is no less criminal, he

says.

The first move a public figure should make is to determine how far the breach has gone, Mr. Mercer says. "This has the potential to harm anyone or anything else in the system."

If you've been hacked, the thing not to do, says Koretz, is what Weiner did. "I would not hire a private investigator, because they wouldn't have access to Twitter's back-end systems or be able to do the kind of forensics to get to the bottom of how it really happened," he says. Hiring a private team, Koretz adds, "is really more about smoke and mirrors than it is about tracking a hacker."

The move suggests "a desire to control the information that might come from an investigation," says Paul Levinson, author of "New New Media." Someone who really wants to get to the bottom of a crime would be more likely to go to law enforcement, or simply to the help function on a website, says Mr. Levinson.

But the help function tactic, he notes, is fraught with its own challenges.

Penny Sansevieri, an instructor at New York University, says she ran into problems trying to follow Twitter's own protocol for hacking. A spammer sent out a single tweet from her account, triggering an account shutdown.

"I went back and forth with [the support team] for about ten days," she says. "My goal was to find out what happened, and most important to get the site back up again," she says. "They did not make this easy at all."

The team even emailed her a response indicating that the event had been resolved, "but it had not, so I had to keep going back to them." Finally, she got her account back. "They made me change the password twice, but they wouldn't tell me why," she says.

Other social media sites have their own ways to make life difficult after a perceived violation, notes Ms. Sansevieri, whose small business Author Marketing Experts relies on social media. One of her authors used a personal Facebook account to post business information, she says, "and Facebook shut it down. No matter what he did, they would not give it back."

Adds Levinson, "It's highly ironic that while we have companies that have become very sophisticated in their rush to be the next big social media, there is no equal rush to provide help in security issues."

"I get better tech help from Sears," he adds.

RELATED: Top 5 most expensive data breaches

Related stories

How attack on Google's Gmail skirted US security roadblocks

Twitter scandal: a mess for Anthony Weiner, a lesson for Congress

How 'cookiejacking' could steal people's Facebook passwords

Topics

Internet • Science and Technology • Technology • Social Software and Tagging • Government and Politics • Politics

Advertisement



"Renegade" trader spills secret to becoming rich with dirt cheap penny stocks...



Alameda - New trick allows many California residents to get car insurance at half-price.



Exclusive short video reveals the secret of how to learn any language in just 10 days!



1 simple rule to making a fortune overnight...

Follow the Monitor on Twitter and Facebook.

Save 57% when you give the Monitor this holiday season!

Read Comments

[View reader comments](#) | [Comment on this story](#)



The advertisement banner features a blue background with a white grid pattern. On the left is the Pardot logo. The main text reads "Automate your lead scoring and nurturing in" followed by "4 Quick Steps" in a larger font. A small orange ribbon with the word "FREE" is positioned above the "4 Quick Steps" text. Below "4 Quick Steps" is the text "a white paper >". On the right side of the banner is an orange button with the text "Download Now!".

© The Christian Science Monitor. All Rights Reserved. [Terms](#) under which this service is provided to you. [Privacy Policy](#).