WikiLeaks, Smart Phones and Email Privacy - What We're Learning

November 4, 2016 - Regardless of which presidential candidate you support, this election cycle has produced some very valuable lessons that everyone should learn when it comes to email privacy. WikiLeaks provided the first lessonâ€¦ that nothing stored or sent electronically is private. More recently, a subpoena for a laptop computer belonging to disgraced former congressman Anthony Wiener provided another lessonâ€¦ that files you may have thought you had deleted can easily and unexpectedly rear their ugly head again if you arenâ€™t careful.

For weeks now, WikiLeaks has been publishing hacked emails from the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC). While the federal government has said that they believe that the hacking was done by Russia, WikiLeaks is saying the feds are incorrect.

Emails stolen in that hack apparently provided enough information to allow the hackers to launch a separate phishing attack against Hillary Clinton's campaign chairman; John Podesta. As a result, they gained access to one of Podesta's accounts and those emails are now being released by WikiLeaks too.

The information contained in the messages from both hacks is more than embarrassing. Some of the messages could lead to criminal prosecutions of people. While many of those individuals may have deleted the computers they used, they had absolutely no control over copies of the messages stored on recipient computers.

In the case of Anthony Weiner's computer, the damage from old emails may be even more extensive. From what we've been able to learn, one of Hillary Clinton's closest aids - Huma Abedin - periodically thought she was backing up the

contact list stored on her smart phone to the computer. But apparently, she never bothered to change the default settings on the backup program she was using. Because of this, every time she backed up her contacts, she also created a backup copy of her email messages. As it turns out, 650,000 email messages wound up being stored on the computer.

Due to a criminal probe, all of those email messages wound up in the hands of the NYPDâ€¦ and eventually in the hands of the FBI. Regardless of their content, this isn't what she had in mind when she was backing up her device.

The lessons here aren't just for individuals. There is a lesson here for corporations too. Any organization that uses or supplies smart phones to their employees needs to make sure that back-up copies of information on those devices is under the control of the organization rather than under the control of individual users. And companies would be wise to develop content and storage guidelines for electronic communications, and provide employee training to ensure those guidelines are adhered to.

We're all tempted to communicate using the easiest method available to us. Often, that means email or text message. But every message sent using one of these methods is vulnerable to hacking and discovery. When dealing with information that you want to handle discretely, your best bet is probably to pick up the phone or meet in person.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS