What to Do if Your Facebook is Hacked

Last week we discussed securing your Facebook, but what should you do if your account does get hacked? You need to regain control as soon as possible because there are several different ways hackers use a breached

Facebook account. Automatic log-ins through Facebook allow hackers access to many different site accounts once they've taken over your Facebook. Spammers also hack Facebook accounts to gain access to your following. From your profile, a hacker can additionally gather a lot of personal information about you that can be used to steal your identity.

If you worry that your account has been hacked, there is a simple way to check. Go to the arrow in the upper right-hand corner of your Facebook page and click on it. In the menu, select **Settings.** A new menu will pop up. Choose **Security and Login** and then **Where You're Logged In**. A list of all of the devices that you've logged into and their locations will pop up. If there is a login you don't recognize, chances are you may have been hacked. If you see anything that isn't you, click **Not You?** on the right side of the log. Then click **Secure Account.** Facebook will then walk you through the steps of securing your account after running a diagnostic on your account.

Facebook takes security very seriously, and they want to hear about it if you've been hacked. If you have a Facebook hacked account and you can't get into your account but you still have access to your email account, Facebook will help you regain access.

The following steps will get you back in control of your account:

1. Go to the [Facebook Account Compromise Reporting Page](#)
2. Click the "My Account Is Compromised" button
3. On the "Identify Your Account" page, enter either your e-mail address, phone number, Facebook username, or your name and the name of one of your friends.
4. Follow the instructions provided to report your account as compromised.

5. Once your account has been reinstated and is back under your control, reset your Facebook password from the "Account Settings" page by clicking the "Change" link under the "My Account" Password section.
6. From the Facebook Privacy Settings page, click on "Apps and Websites". Under the "Apps, You Use" section, click "Edit Settings" and then click on the "X" to delete any suspicious/malicious apps that may have been used to compromise your account.
7. Alert your friends that your account was hacked and warn them not to click on any links that the hackers who compromised your account may have posted on their walls, in chat sessions, or in Facebook e-mails that the hackers sent to them.

Again, to help prevent this from happening in the future, consider enabling features such as Facebook Login Approvals and any other Facebook authentication approval process that relies on multiple authentication factors.

This Week's Cyber Alerts:

Alert Issued 2/9/18 **73 Percent of Firms Fail Cybersecurity Readiness Tests**

Alert Issued 2/9/18 **2017 Smashed World's Records for Most Data Breaches, Exposed Information**

Alert Issued 2/8/18 **Hacker Easily Bypasses Windows 10 Anti-ransomware Protection with this Trick**

Alert Issued 2/8/18 **42 Percent of the Most Popular Websites are Vulnerable to Cyberattacks**

Alert Issued 2/7/18 **Hackers Crack Smartphone Location Tracking â€" Even if You've Turned Off the GPS**

Alert Issued 2/5/18 [Microsoft goes after Windows Scareware that tries to Pressure You for Payment](#)

Alert Issued 2/2/18 [Fake tax returns? How Equifax, Data Breaches Increase the Risk of Fraud](#)

Alert Issued 2/1/18 [Millions of Fortune 500 Email Credentials Found on the Dark Web](#)

Thank you for subscribing to our email and I hope the information we have shared will make your online life a little easier.

Home Cyber Defense Weekly is a service of House of File Technologies