proofpoint.

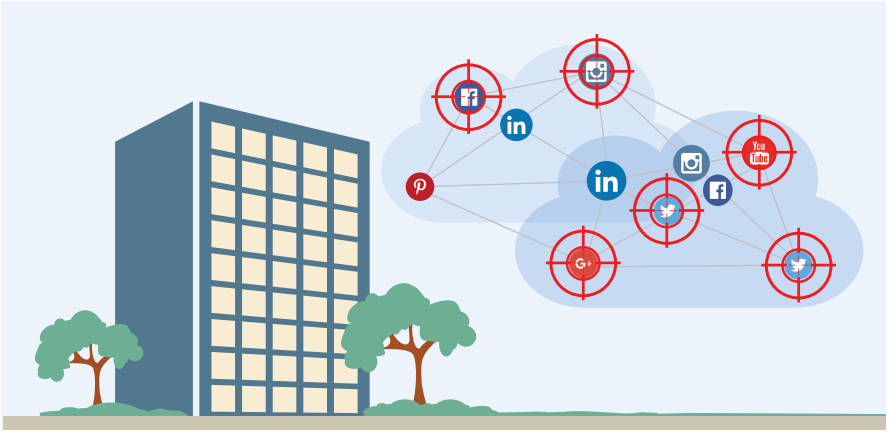
SOCIAL MEDIA ACCOUNT TAKEOVERS

Companies are engaging customers on social media more than ever. It's no wonder that cyber attackers see prominent social accounts as a ripe target. Account takeovers have become synonymous with embarrassing headlines that feature prominent companies and figures.

Most organizations lack the protective countermeasures or the expertise to mitigate risk and respond to these incidents. Few companies know how to regain control after an account compromise—or how to prevent an attack in the first place.

HOW ARE THE TAKEOVERS POSSIBLE?

Details of social media account takeovers are often oversimplified. Many think it's only a matter of mismanaged passwords. But the reality is often more complex. Most companies have a high number of social accounts with complex operating environments. These environments sit outside of companies' traditional infrastructure, out of their IT department's direct control. As a result, they typically lack the security controls that apply to their website and email systems.



COMPLEXITY IS THE KEY

The average enterprise brand has hundreds of social media accounts across social platforms, including Twitter, Facebook, YouTube, and others. And they typically have several dozen admins with account login and publishing privileges. In addition, they often authorize multiple publishing applications to connect to their social accounts to create and communicate content. And there are a lot to choose from—the publishing ecosystem includes more than 20,000 unique apps.

Organizations use an average of 10 unique apps on their Twitter accounts and six apps on Facebook. Companies with very active social feeds can have as many as 35 authorized publishing apps on a single Twitter account. This introduces a high level of risk; each admin and authorized publishing app becomes part of the attack surface for each social account. Bad actors phish account admins for social page or app credentials. Attackers may even use a malicious mobile app to gain access.

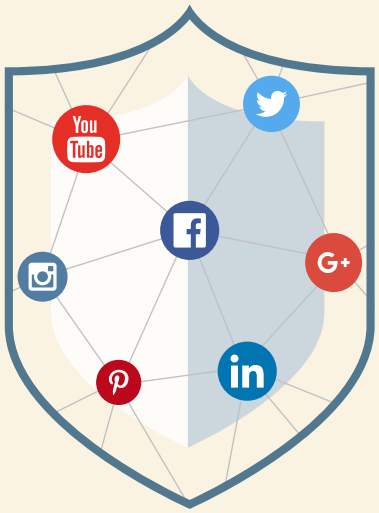
Without the proper security controls in place, this complexity makes it difficult to detect a compromise until it is too late. For example, enterprise brand accounts make up to 50 changes a day on the authorized apps, admins, descriptions, and pictures—in addition to the high volume of content posted.

REDUCING THE RISK OF ACCOUNT TAKEOVERS

Here are seven ways marketing and security teams can reduce the risks of someone hijacking their social media accounts:

1. **Implement access management, strong passwords, and two-factor authentication**
   Shared passwords, dormant users, weak passwords, and manual password tracking increase your company's exposure to social account takeovers. Only users with a business need should have access to your accounts, and they should be subject to strong password policies. Ideally, you should adopt two-factor authentication as well. Use Proofpoint Password Lockbox to streamline how you manage access rights and implement a strong password policy. With this step, you can stop sharing passwords over email or spreadsheets. You can also integrate Password Lockbox with two-factor authentication.

7 BEST PRACTICES TO REDUCE THE RISKS OF SOCIAL MEDIA ACCOUNT TAKEOVERS.



2 Audit your publishing apps

So many apps are inadvertently granted approval to connect and publish to your social media accounts. Use Proofpoint Social Patrol to audit all the apps that have been granted access and de-authorize those that shouldn't. Then use Proofpoint App Policies to monitor for any new unauthorized access that may appear over time. We detect when a new publishing app connects to your account and send you an alert to approve or lockdown the app if it has been compromised.

3 Automate locking your social account

If your account is compromised, deploy technology that automatically locks your account to stop the attacker from doing further damage. Proofpoint ProfileLock takes a snapshot of your account information and monitors the account for any account changes or anomalous activity. If it detects anything, you get an alert and can automatically lock down your account to prevent future publishing. Watch the video demo here.

4 Establish a process to stop new content posts

If your account is compromised, the last thing you want is for your apps to continue churning out bad content. Disabling any application capable of spreading the negative content will help you avoid further damage. Proofpoint SocialPatrol can help. Our "Block All Apps" policy automatically deletes any new content posted to the compromised account. Use this technique to temporarily stop all activity across any number of accounts.

5 Suspend your account

If you cannot recover the account by resetting passwords, contact the platform immediately to suspend the account. Here is a list of ways to contact some of the leading social networks:

- Facebook report a hacked account
- Twitter support request
- Google+ account recovery
- YouTube hacked account
- Instagram hacked accounts
- Pinterest account security
- LinkedIn report a hacked account

6 Develop and test your response plan

Develop a plan for responding to account takeovers. It should include pre-defined messages that let your stakeholders know the actions you've taken, the procedure to follow, and the correct messages for the press. It should also include procedures for escalating issues and communicating with customers. Then test your plan. Run a "red team" exercise that improves its effectiveness.

7 Create a response web page

Create a hidden web page with a shortened link that is pre-approved and ready if an event occurs. The page should have a basic template in place that you can quickly modify with the proper response. This link can then be shared across the appropriate channels to drive a clear and consistent message.

We are here to help. As a recognized leader in protecting media and large brands from social media account hacks, we can help you mitigate the downstream impact of multi-channel credential phishing.

Click here for more information on how to protect your accounts