WHITE PAPER

proofpoint™

HOW TO STOP SOCIAL MEDIA HACKS

TABLE OF CONTENTS

HOW TO STOP SOCIAL MEDIA ACCOUNT HACKS

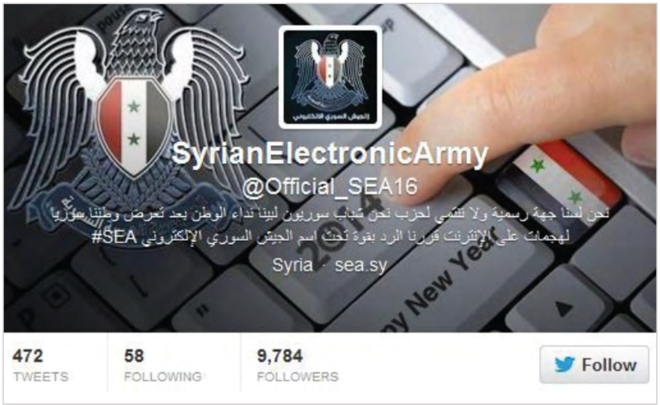
The words “social media hack” have become synonymous with embarrassing headlines. These articles feature prominent companies and figures that have fallen victim to misuse of their social channels.

Social media has risen in popularity and hackers see prominent social accounts as a ripe target. The social networks of Burger King, Associated Press, Jeep, and even President Obama have all been splayed open by hackers, exposing them to public humiliation. Within hours of ringing in the 2014 New Year, both Skype and Snapchat suffered hacking attacks.

Little has been done to address the hacking problem despite continued headlines. Most organizations lack the protective countermeasures or the expertise to mitigate risk and respond to incidents. Few companies know how to re-gain control after an account compromise or how to prevent an attack in the first place.

Most often, prevention efforts rely solely on the controls available within the social media platforms. These controls include two-factor authentication, Secure Sockets Layer (SSL) encryption, or manual review of comments and posts.

These built-in security systems have their own set of problems and do little to mitigate hacking risks. For example, two-factor authentication is not universally available and does not operate on a per user basis. This means that accounts with multiple administrators remain vulnerable. Many corporate accounts have multiple administrators and are exposed to this risk. Likewise, SSL encryption does not address the hacking problem. It is designed to secure communications in a web session rather than prevent an unauthorized user from accessing an account. Manual content filtering is simply unsustainable. Not only is it inefficient and prone to human error, it is also tremendously resource intensive.



SyrianElectronicArmy

@Official_SEA16

نحن لسنا جهة رسمية ولا ننتمي لحزب نحن شباب سوريون لبينا نداء الوطن بعد تعرض وطننا سوريا
لهجمات على الإنترنت قررنا الرد بقوة تحت اسم الجيش السوري الإلكتروني #SEA

Syria · sea.sy

Additionally, poor password management is common for social media managers and puts companies at risk. Typical mistakes include storing credentials in Excel and sharing passwords with colleagues.

Despite hacking risks, organizations embrace social media as an essential tool in their marketing and communications strategies. Companies continue to invest resources to build up their social infrastructure. U.S. brands will spend an estimated $35.98 billion on social advertising in 2017. This unguarded influx of money has created a hacker’s dream. All attackers need is a simple password to turn a social infrastructure investment into a moneymaking opportunity.

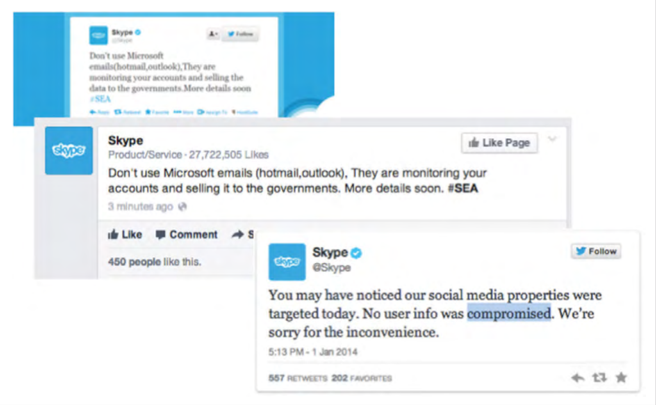
HACKER TECHNIQUES, DETECTION, AND PREVENTION METHODS

Facebook, YouTube, Twitter, and the other social networks have tools in place to detect and defend against direct hacking attempts. The most common methods hackers use to gain access to accounts is through poorly maintained passwords, authorized users, and compromised applications.

POOR PASSWORD MANAGEMENT

Looking at today's social media password management is like stepping back to email security in the '90s. Departments share passwords, dole out administrative access like candy, and keep credentials stored openly on Post-Its.

A seemingly "advanced" organization might have an Excel file containing a list of everyone who has access, including usernames and passwords. They often email or IM the forgotten passwords or store the Excel file on a shared drive.



Skype @Skype

Don't use Microsoft emails(hotmail,outlook),They are monitoring your accounts and selling the data to the governments.More details soon #SEA

Skype
Product/Service · 27,722,505 Likes

Don't use Microsoft emails (hotmail,outlook), They are monitoring your accounts and selling it to the governments. More details soon. **#SEA**

3 minutes ago

450 people like this.

Skype
@Skype

You may have noticed our social media properties were targeted today. No user info was compromised. We're sorry for the inconvenience.

5:13 PM - 1 Jan 2014

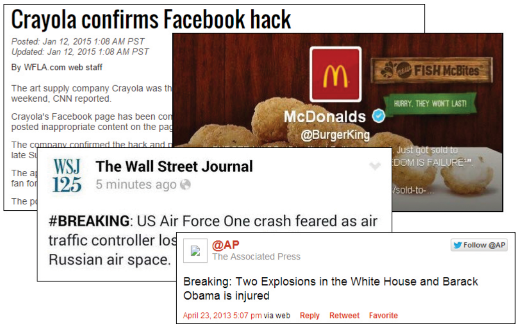
557 RETWEETS 202 FAVORITES

Employees come and go. They often maintain access to your accounts even after they leave. This is especially common when their access was established through their personal social media account. Your PR and marketing firms also share access with their employees, many of whom you will likely never know or meet.

Bottom line: we can all acknowledge the lack of security on social media. It's only a matter of time before someone loses the password list or gets infected with malware that steals the stored passwords. It is almost inevitable that a current or former administrator will publish something inappropriate on your corporate page. It might be an accident, or it might be a revenge attempt from a disgruntled employee. No matter how it happens, an account hack can have lasting consequences for your company.

Organizations need to look beyond the common misconception that a social media publishing tool will solve the password access problem. No single marketing tool should completely manage access. Additionally, employees have good reasons to use the social platform's native functionality. They may need to pin a post or buy paid ads. Your organization needs more than a publishing tool. You need a way to manage access to your social accounts.

If the problem is understood, why aren't organizations addressing the access issue? The answer is simple: most marketing, security, and compliance personnel don't think there a solution exists. In fact, the solution is simple.



Crayola confirms Facebook hack

Posted: Jan 12, 2015 1:08 AM PST
Updated: Jan 12, 2015 1:08 AM PST

By WFLA.com web staff

The art supply company Crayola was th
weekend, CNN reported.

Crayola's Facebook page has been com
posted inappropriate content on the pag

The company confirmed the hack and
late Su

The ap
fan for

The p

McDonalds
@BurgerKing

Just got sold to
DOM IS FAILURE".
/sold-to-...

The Wall Street Journal
5 minutes ago

#BREAKING: US Air Force One crash feared as air traffic controller los
Russian air space.

@AP
The Associated Press

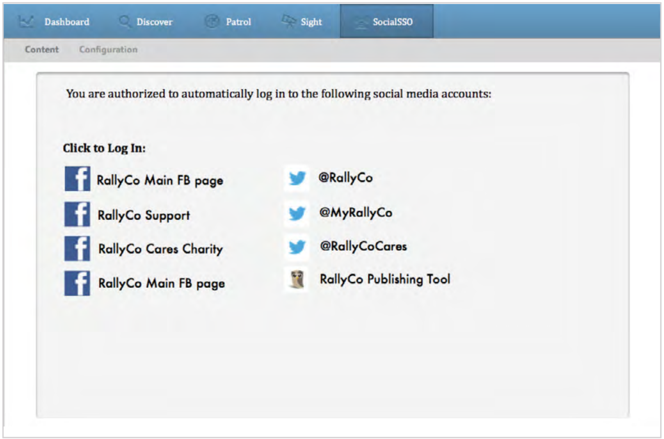
Breaking: Two Explosions in the White House and Barack Obama is injured

April 23, 2013 5:07 pm via web Reply Retweet Favorite

First, you should stop giving employees and partners direct access to your social media accounts and marketing applications. Instead, you should adopt Single Sign-On (SSO) technology that integrates with your corporate directory services (e.g., LDAP). Using SSO, you can automatically identify users and groups. Then you can provision access based on policy (e.g., the social media team can access your social media publishing tool).

SSO technology acts as an interface between your employees and your accounts. Instead of giving all your account and application passwords to every employee who needs access, you store your credentials in the SSO solution. Then, your employees create their own username and password for the SSO solution. When they log in via SSO, they will only have access to the accounts and applications they are authorized to use. Changes to a user's access can be controlled centrally without changing account passwords.

With this process, your uses don't need to remember multiple usernames or passwords. When employees join or leave your organization their access is added or removed from your social cannels and marketing apps—just as they are added to or removed from your corporate directory services.



You are authorized to automatically log in to the following social media accounts:

Click to Log In:

RallyCo Main FB page
RallyCo Support
RallyCo Cares Charity
RallyCo Main FB page

@RallyCo
@MyRallyCo
@RallyCoCares
RallyCo Publishing Tool

Following these steps reduce your risk of a security threat, hack, and employee misuse of your accounts:

1. Adopt a social media security solution that includes user authentication and access management for social media platforms and applications.
2. Work with your IT department to identify groups or users within your directory services infrastructure who should have access to your social accounts.
3. Map the employees and partners to the applications to which they should have access. Create and apply those profiles and mappings in your social media security tool (e.g., social response team can access listening and publishing tools).
4. Don't give out direct access to your social media accounts and applications. If you have in the past, rescind access and notify your employees and partners.
5. Make sure your employees know not to share their credentials and why. Education is a cornerstone of good security practice.

Proofpoint Password Lockbox helps administrators streamline and centrally manage secure access controls to your brand's social media accounts. Simply provision and de-provision user access and seamlessly monitor and manage who can access which social accounts.

Password Lockbox reduces your attack surface by ensuring users never have administrator-level passwords. Your employees and partners get protection from fraud and spear fishing attacks, and hackers can't obtain the credentials to directly access your brand's social accounts.

PHISHING ATTACKS

Phishing attacks usually seek financial or confidential information and appear to come from a legitimate sender. For example, the hacker sends a message that appears to be from Facebook asking the recipient to “log in” to or “authorize” the social media account. The user, who thinks she is logging into her Facebook account, enters her username and password into a fake login page, which captures the credentials and passes them to the hacker.

Phishing attacks are highly targeted. Hackers will use social media to identify who the administrators are for your branded accounts and then use email and/or direct messaging to target them.

Follow these three steps to prevent a phishing attack:

1. Limit the number of administrators and applications that have authorized access to your social media accounts. This helps minimize your attack surface. Use a password management solution, such as Proofpoint Password Lockbox, to ensure your employees and partners don’t have the root credentials to your social media accounts and applications.
2. Educate your account administrators on phishing attacks that request their login credentials. Never click on links in these emails or messages. Instead, administrators should use their web browser to navigate directly to their social media account. If the account requires a password change or re-authorization, it will prompt the user on the webpage directly.
3. Ensure your administrators use strong passwords and that they are always different from their personal or corporate usernames and passwords. If there are too many passwords to remember, consider using a secure password vault such as LastPass, Proofpoint, or OneLogin. These tools provide an added verification benefit; they will only automatically fill in information on legitimate sites.

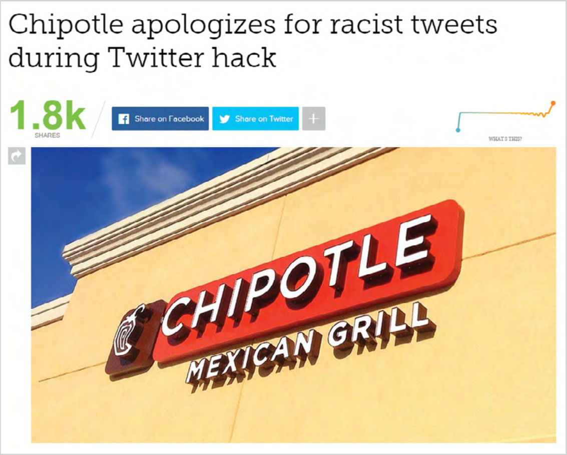
Some phishing attacks are successful and lead to an account takeover. Proofpoint ProfileLock detects account hacks and enables administrators to lock down hacked accounts. The solution takes a snapshot of preferred account settings and notifies administrators of account changes. ProfileLock looks for account changes to privileges, administrators, descriptions, profile photos, links, emails, and more. If the account is compromised, ProfileLock can also automatically remove unauthorized content.

BROWSER AND COOKIE ATTACKS

Social networks are designed to keep you logged in. Connections to your social media networks don't time out because they use an authentication cookie. However, keeping a browser session open provides the perfect avenue for hackers to access your social media accounts.

These cookies are easily intercepted when you connect to open Wi-Fi networks. If an attacker intercepts the cookie from one of the social networks, he can post or make changes with the same permissions of the logged in administrator.

If your administrator logs into your corporate Facebook page from a shared computer and forgets to log out, the next user of that computer can makes changes to your account and publish to your page.


Chipotle apologizes for racist tweets during Twitter hack

1.8k SHARES

Additionally, if an administrator inadvertently visits a page infected with malware and has a browser open to your branded Facebook or YouTube account, the hacker may be able to inject content onto your page via the open browser session.

Browser attacks are either very targeted or not at all. A targeted browser attack is typically a combination of a phishing scheme and a generic browser attack via malware. However, a non-targeted attack usually circulates in a mass email or hacked website that your administrator randomly encounters. You can defend against non-targeted attacks with consistent security training.

To prevent targeted browser and cookie attacks, follow these five steps:

1. Ensure administrators only access your social media accounts from trusted machines and require them to log out after each session.
2. Ensure administrators always use secure connections (i.e., HTTPS) when logging in.
3. Use authorized publishing, listening, and other social media tools to access your social media accounts. Do not directly login to social media networks, unless necessary. When you must login directly, use a trusted and clean computer.
4. Ensure your administrators use trusted devices to access your social accounts and that the devices are running up-to-date anti-malware software.
5. Use Proofpoint ProfileLock to get an overview of your accounts, receive alerts when changes are made, and automatic removal of unauthorized content in the event of a hack.

For a complete description of roles and responsibility management for social media security and compliance, read our paper here:
go.proofpoint.com/roles-and-responsibilities-for-social-media-risk-management.

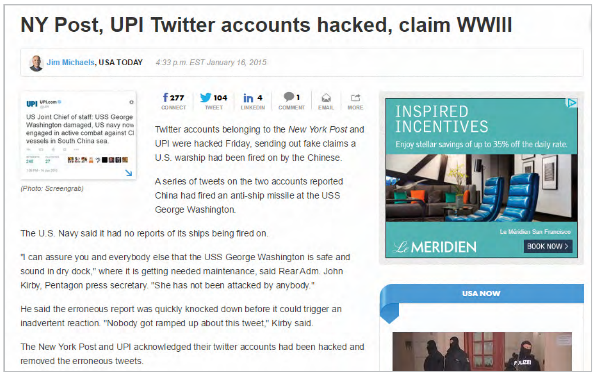
HOW TO SECURE YOUR SOCIAL MEDIA ACCOUNTS

Collaboration between social media and security teams helps prevent social media account hacks. While the onus of protecting a brand's accounts ultimately falls on IT security, inter-department coordination provides greater visibility into how the company is engaging on social media and helps define required protection measures.

There are many people, process, and technology safeguards brands can implement to protect themselves and their followers. As a start, here are three steps you can take:

KNOW YOUR BASICS

It's important to have a full understanding of your social account footprint. You need to find all your social accounts before you can protect them. Identify your primary and secondary accounts, as well as the stakeholders responsible for managing each of them. You should designate a primary account holder and a crisis communication team. In doing so, you'll create a working committee that fosters a culture of awareness and open interaction across departments. This will help you protect your brand from hackers.



NY Post, UPI Twitter accounts hacked, claim WWIII

Jim Michaels, USA TODAY 4:33 p.m. EST January 16, 2015

UPI UPI.com

US Joint Chief of staff: USS George Washington damaged, US navy now engaged in active combat against Cl vessels in South China sea.

(Photo: Screengrab)

Twitter accounts belonging to the *New York Post* and UPI were hacked Friday, sending out fake claims a U.S. warship had been fired on by the Chinese.

A series of tweets on the two accounts reported China had fired an anti-ship missile at the USS George Washington.

The U.S. Navy said it had no reports of its ships being fired on.

"I can assure you and everybody else that the USS George Washington is safe and sound in dry dock," where it is getting needed maintenance, said Rear Adm. John Kirby, Pentagon press secretary. "She has not been attacked by anybody."

He said the erroneous report was quickly knocked down before it could trigger an inadvertent reaction. "Nobody got ramped up about this tweet," Kirby said.

The New York Post and UPI acknowledged their twitter accounts had been hacked and removed the erroneous tweets.

Take stock of both your company and employee-owned accounts when you begin your account search. Employees often create accounts for themselves or on behalf of your organization (e.g., affiliated with a particular region or product, etc.) unbeknownst to the brand manager or corporate communications team. These accounts may be active or orphaned, but are often widespread. Although your organization may have its list of "official" accounts, a hacker targeting an unknown or unofficial page can still do a lot of damage.

Manual searches across all major social networks can be a time consuming effort. We recommend that you automate the search process with technology that also provides recurring scans. This is important as new accounts may be created at any time and by any one. Once you have an inventory of your accounts, identify everyone who has login access to both your accounts and applications. Confirm that each user's access is authorized. Work with your IT team to integrate a social media security tool to govern who can access which social platforms and apps. This will also allow you to automate seamless provisioning and de-provisioning.

PREVENT AND DETECT

Reduce the number of direct administrators for each account; strengthen your passwords, and use password management solutions. These simple steps can make a big difference in minimizing risk. Weak passwords create vulnerability. With your brand's reputation at stake, it is worth the effort to amp up your basic security measures. Create a strong, complex password and regularly refresh it to make it difficult for hackers to access your account. Make sure your users do not self-manage passwords or have direct access to your social accounts and apps. Instead, manage access via your SSO tool — just as you govern access to the rest of the applications your organization uses (e.g., email, IM, corporate network access, etc.).

Giving more people access to your accounts makes it easier for an unauthorized party to gain access. Every employee with direct access is a prime target for phishing attacks, so be selective. Limit the number of people who can perform key activities that open your company up to risk, such as installing apps or authorizing a mobile device.

You can limit the number of users that have access to your brand's social media accounts with planning and technology. Using an SSO solution like Proofpoint Password Lockbox, you can create roles and policies for access.

Roles let you decide who is responsible for managing and protecting your social infrastructure. This infrastructure includes installed apps and account configurations, media and ad purchases, and social engagement tools. Despite the need for direct account access, SSO technology mitigates the need for users to have, know, and use credentials that directly access the accounts and apps.

Third party applications often go hand-in-hand with social media use. While great for promotional capabilities, they can also introduce risk. Social media apps connect to your accounts via the authorization of an access token. These tokens often provide read and write access to comments and posts—access that indefinite unless revoked. If an application's access token database is unencrypted, hacked, or stolen, an attacker can pass the token over to the platform's API and gain access to the account.

To mitigate this risk, reduce the number of apps installed on your account and the number of users with access. Ideally, your organization should only use three to six connected apps at one time. These could include a publishing app; customer support / CRM, or community management app; a photo / video sharing app; an ad or content placement platform; a designated mobile content publishing app (if different from your primary publishing app); and your security app.

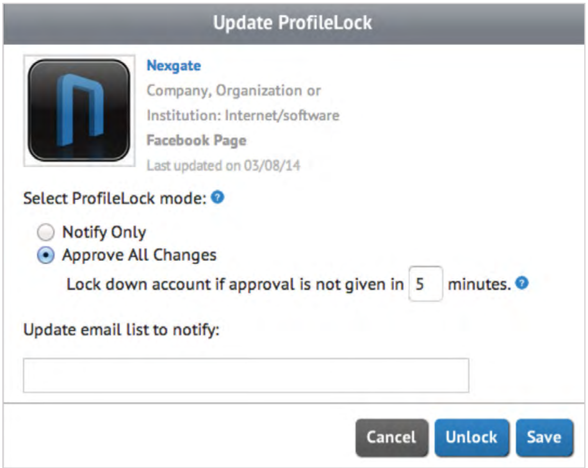
Use social media security technology to automatically limit the apps authorized to publish on your behalf and to ward off the risk of an admin mistakenly installing an unauthorized application. Choose a solution that can also monitor your accounts for anomalies that are indicators of a hack. Automated monitoring is especially important for secondary accounts where day-to-day governance may not be as tight as it is on your primary accounts. While manual monitoring of accounts for warning signs is certainly valuable, implementing automated technology improves accuracy and expedites the process, saving you valuable time and resources.

IF A HACK DOES OCCUR, RESPOND IMMEDIATELY

If your account is compromised, immediately lock down all your publishing apps. The last thing you want is for your publishing platforms to continue churning out bad content. Disabling any application capable of spreading the negative content will help you avoid further damage.

In the aftermath of a hack, you should also take swift action to remove the unwanted content. The best way to do this is through automated technology, which takes immediate action to address the problem and put your social accounts back on the right track.

Next, contact the social platforms and regain total control. Here is a list of ways to contact some of the leading social networks:



Update ProfileLock

Nexgate
Company, Organization or Institution: Internet/software
Facebook Page
Last updated on 03/08/14

Select ProfileLock mode:

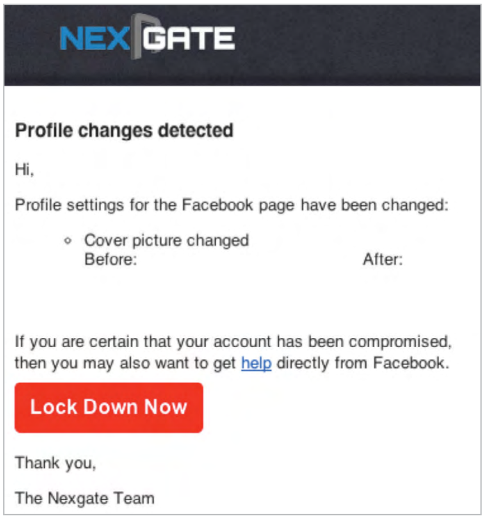
○ Notify Only
● Approve All Changes
Lock down account if approval is not given in 5 minutes.

Update email list to notify:

1. Facebook report a hacked account: www.facebook.com/hacked
2. Twitter support request: support.twitter.com/forms/signin
3. Google+ account recovery: www.google.com/accounts/recovery
4. YouTube hacked account: support.google.com/youtube/answer/76187?hl=en
5. Instagram hacked accounts: help.instagram.com/368191326593075
6. Pinterest account security: en.help.pinterest.com/forums/21100817-Account-Security
7. LinkedIn no access to primary email address: help.linkedin.com/app/answers/detail/a_id/1501

Create and implement a clear communications plan for the smoothest post-hack recovery. This plan should be cover both your employees and the media. It's important for your company to run as cohesively as possible following a security event. Your communications plan is critical to unify your response and ensure your team members know their role in the recovery effort.

While there may be no such thing as an impenetrable social media account, the above steps will strengthen your company's social fortress, remove vulnerabilities, and help you efficiently respond to an attack.



Profile changes detected

Hi,

Profile settings for the Facebook page have been changed:

- Cover picture changed
  Before: After:

If you are certain that your account has been compromised, then you may also want to get help directly from Facebook.

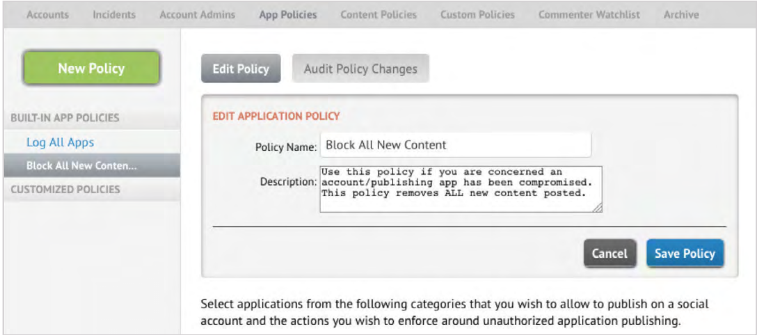
Thank you,

The Nexgate Team

SIX STEPS TO STOPPING AN ACCOUNT HACK WITH PROOFPOINT

If you do have a breach, here are some best practices collected from Proofpoint Social Media Protection customers:

1. Establish access roles and privileges with Proofpoint Password Lockbox. This streamlines password management, eliminates shared passwords, and removes direct credential access to your social media accounts and applications.
2. "Lock" the account via the Proofpoint ProfileLock email alert or in the ProfileLock user interface. ProfileLock takes a snapshot of your account information and alerts you when there's a change. ProfileLock will also lock down your account and prevent future publishing should an unauthorized change occur. Watch the video demo here.
3. Select the "Block All Apps" policy for any compromised accounts. If the breach is likely to spread, use this technique to temporarily stop all activity across accounts.
4. If you cannot recover the account by resetting passwords, contact the platform immediately to suspend the account.
5. Develop an internal communication system and pre-defined messages that let your stakeholders know about the situation. These notifications should include the actions already taken, the procedure to follow, and the correct messages for the press.



EDIT APPLICATION POLICY

Policy Name: Block All New Content

Description:
```
Use this policy if you are concerned an
account/publishing app has been compromised.
This policy removes ALL new content posted.
```

Select applications from the following categories that you wish to allow to publish on a social account and the actions you wish to enforce around unauthorized application publishing.

6. 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.

[1] Social Network Ad Spending: www.emarketer.com/Article/Social-Network-Ad-Spending-Hit-2368-Billion-Worldwide-2015/1012357

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.