Defense Media Activity

Guide To Keeping Your Social Media Accounts Secure

TABLE OF CONTENTS

PROTECTIVE MEASURES 3
PREPARATION CHECKLIST 3
TWITTER 4
FACEBOOK 5
GOOGLE + AND YOUTUBE 6
PROHIBITIVE MEASURES 6
INSTAGRAM 7
FLICKR 7

Social media is an integral part of the strategic communications and public affairs missions of the Department of Defense. Like any asset, it is something to defend and protect with vigilance. Cyber attacks are a real and present threat to the cyber security of government social media accounts. In this guide you will find the steps and contacts needed in order to be protective, preventative, prohibitive and proactive against cyber-attacks.

If you suspect that your organization is being targeted or compromised by a malicious cyber-attack, you must be proactive and swift to mitigate this threat. The steps you take can help to greatly reduce the risk of exposure and vulnerability of attack to your organization.

PROTECTIVE MEASURES

Use a strong password. At least 20 characters long, that is either randomly-generated (like LauH6maicaza1Neez3zi) or a random string of words (like “hewn cloths titles yachts refine”). Use a unique password for each website or service you use; that way, if one account gets compromised, the rest are safe.

Use a government e-mail address, also with a strong password. A .gov or other private-domain account will generally be more secure than a public service, and will reduce the possibility of password-reset and other emails being intercepted. If you must use a public email provider, consider added precautions such as Gmail’s two-factor authentication.

Don’t give your username and password out to untrusted third parties, especially those promising to get you followers or make you money.

Select third-party applications with care. There are thousands of applications built by external developers that allow you to do an array of neat things with your account. However, you should be cautious before giving up control of your account to someone else. Revoke access for any third-party application that you don’t recognize by visiting the Applications tab in your account settings.

Make sure your computer and operating system is up-to-date with the most recent patches, upgrades, and anti-virus software, and that all your computers and mobile devices are protected by secure passwords.

PREPARATION CHECKLIST

Change your Twitter account passwords. Never send passwords via email, even internally.

Keep your email accounts secure. Twitter, Facebook, Google+, etc use email for password resets and official communication. Change your email passwords, and use a password different from your social media account passwords.

Review your authorized applications. Log in to Twitter or Facebook and review the applications authorized to access your accounts. If you don’t recognize any of the applications on Twitter, contact

them immediately by filing a security ticket and emailing hacked@twitter.com.

Use extra security features. This will help keep your accounts protected. **Facebook has a whole section on how to do that located here**.

Build a plan. Create a formal incident response plan. If your organization is a target for a phishing campaign or has been hacked, you'll be prepared to take action and resolve the issue immediately.

Talk with your security team about ensuring that your email system is as safe as possible.

Minimize the number of people who have access to the account. Even if you use a third-party platform to avoid sharing the actual account passwords, each of these people is a possible avenue for phishing or other compromise.

Log out of Facebook and Twitter when you use a computer you share with other people. If you forget, you can log out remotely.

Check for signs of compromise. Checking your email address and authorized apps weekly or monthly can help detect unauthorized access and address the problem before access is abused.

Change your password regularly. Changing your social media passwords quarterly or yearly can reset the clock if a password has leaked.

Using a Password Manager integrated into your browser can help prevent successful phishing attacks. Third-party solutions such as **1PASSWORD** or **LASTPASS** make it much easier to use a very strong password. Password managers, as well as the browser's built-in password manager, will only auto-fill passwords on the correct website. If the password manager does not auto-fill, this might indicate a phishing attempt.

IF YOU SUSPECT YOUR ACCOUNT IS COMPROMISED, THE FOLLOWING ACTIONS ARE ADVISED:

1. Notify your chain of command immediately
2. If possible, suspend all accounts to prohibit further illicit activity
3. Take the following action on the following platforms to stop the hack from proceeding

TWITTER

If you suspect your organization is being targeted by a phishing campaign or has been compromised by a phishing attack, contact us immediately at hacked@twitter.com with the word "Hacking" in the subject. Include copies of suspected phishing emails.

1. **Immediately change your Twitter password and the password** on the email associated with the account, following the tips at right.
2. Delete any unwanted Tweets that may have been sent without your permission.
3. Go to the Applications tab of your account settings and revoke access to any apps you don't recognize. To be absolutely sure, revoke them all and reauthorize known apps and devices by logging in from them one-by-one.
4. You should also check the Mobile tab of your account settings. If the phone number associated with the account is not yours, click the "Delete my phone" link at the bottom of the page.
5. Remind anyone with authorized access to your account to follow the precautions outlined on this page.
6. If you can't access your account, file a support ticket at **https://support.twitter.com/forms/hacked** and email the ticket number to hacked@twitter.com.

FACEBOOK

If you suspect your organization is being targeted by a phishing campaign or has been compromised by a phishing attack, contact them immediately at **Katie.Harbath@fb.com** (government Facebook representative) to explain the situation.

If you think your account was taken over by someone else, Facebook can help you secure it. This process can also help if your account or computer has been affected by a virus or malware.

For more information about staying safe on Facebook, please visit the Security Page or our Help Centre.

Here are a few things you can do to keep your account safe:

- **Pick a unique, strong password.** Use combinations of at least 6 letters, numbers and punctuation marks and don't use this password for any of your other accounts. You can also use a password safe like **LASTPASS**, **KEEPASS** or **1PASSWORD** to set and remember unique passwords for your account. Learn how to **change your password**.
- **Think before you click.** Never click suspicious links, even if they come from a friend or a company you know. This includes links sent on Facebook (ex: in a chat or story) or in emails. If one of your friends clicks a spam link, they could accidentally send you or tag you in spammy posts. If you see something suspicious on Facebook, **report it**. You also shouldn't download things (ex: a .exe file) if you aren't sure what they are. Learn more about**recognizing suspicious emails**.
- **Watch out for fake Pages and apps/games.** Be suspicious of Pages promoting offers that are too good to be true. If in doubt, check to see if a Page is **verified**. Also be mindful when you install new apps or games. Sometimes scammers use **bad apps and games** to gain access to your Facebook account.
- **Don't accept friend requests from people you don't know.** Sometimes scammers will create fake accounts to friend people. Becoming friends with scammers allows them access to spam your Timeline, tag you in posts and send you malicious messages. Your real friends may also end up being targeted.

- **Never give out your login info (ex: email address and password).** Sometimes people or pages will promise you something (ex: free poker chips) if you share your login info with them. These types of deals are carried out by cybercriminals and violate the **Facebook Statement of Rights and Responsibilities**. If you're ever asked to re-enter your password on Facebook (ex: you're making changes to your account settings) check to make sure the address of the page still has facebook.com/ in the URL (web address).
- **Log in at www.facebook.com.** Sometimes scammers will set up a fake page to look like a Facebook login page, hoping to get you to enter your email address and password. Make sure you check the page's URL before you enter your login info. When in doubt, you can always type facebook.com into your browser to get back to the real Facebook. Learn more about **phishing**.
- **Update your browser.** The newest versions of internet browsers have built-in security protections. For example, they might be able to warn you if you're about to go to a suspected phishing site. Facebook supports:
  - » **Mozilla Firefox**
  - » **Safari**
  - » **Google Chrome**
  - » **Internet Explorer**
- **Run anti-virus software.** To protect yourself from viruses and malware, scan your computer. You can learn more and download this software for free:
  - » **For Windows**
  - » **For Mac OS**

GOOGLE + AND YOUTUBE

If your Google + and/or YouTube account has been hacked, you will need to take immediate action. Change the password for this platform immediately (through Google +).

Contact the government account reps at Google to inform them of the hack: cfincham@google.com or yt-hijack@google.com

PROHIBITIVE MEASURES

Recommend added precautions such as **Gmail's two-factor authentication**.
Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help keep bad guys out, even if they have your password.
An extra layer of security. Most people only have one layer – their password – to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account.

Sign in will require something you know and something you have. With 2-Step Verification, you'll protect your account with something you know (your password) and something you have (your phone or Security Key).

Verification codes made just for you. Codes are uniquely crafted for your account when you need them. If you choose to use verification codes, they will be sent to your phone via text, voice call, or our mobile app. Each code can only be used once. See **Features** to learn about backup options for times when your phone is not available.

For more information, and to get access to the steps you might need to take if your account is compromised, here is the **Google Safety Center link**.

INSTAGRAM

If you think your account has been hacked and you're no longer able to log in, **let Instagram know**.
If your account is leaving comments or sharing things that you haven't posted, your password may be compromised.

To secure your account:

- **Change your password** or send yourself a **password reset email**
- **Revoke access** to any suspicious third-party apps

Note: Never grant third-party access to a website or apps that aren't following our **Community Guidelines** or **Terms of Use** (including websites selling or promising free followers or likes), as it's likely an attempt to use your account in an inappropriate way.

FLICKR

Flickr is a photo and video-sharing community run by Yahoo. Millions of members from all over the world are uploading photos and video that they have created, each sharing their unique view of the world. When using Flickr you can post, sort, and share photos and videos you have created with friends, family, and folks from across the globe.

How to customize your privacy controls: Flickr empowers the community to control access to content by providing multiple options for adjusting privacy settings on photos, your Flickr profile, and even on commenting and contact preferences. To review these settings, visit your **Flickr account page**. Some important sections:

4. Profile settings. You can control your **profile privacy settings** to dictate who is able to see different parts of your profile.

Change a password. For a Yahoo account, you can change your password at https://edit.yahoo.com/config/change_pw. If you can no longer access your account, you can get a new password at https://edit.yahoo.com/forgotroot/.

Commenting controls. You control who can comment on your public photos and videos. By default, anyone is able to comment on your photos. You can change this in the privacy setting for comments. If someone posts a comment you don't like, you can just delete it.

Post with care: The Flickr community is ever growing. As you upload content, be sure to know which privacy settings you have selected and how visible the content will be to the general public. You can also choose to opt out of your content being searchable on third-party sites.

Block unwanted individuals: Sometimes we just don't want to interact with someone. By blocking a community member, that person can no longer interact with you or your photos. There are three ways to block a person:

1. Click the **"Block [membername]"** link on the Person menu.
2. Click the **"Block this person?"** link on the person's profile page.
3. Delete a comment on one of your photos. (You'll see the option to block the person, too.)

To see the people you've blocked, click the link at the bottom of your contact list.

SafeSearch: You can control what kind of content shows up on your Flickr searches. By default, SafeSearch is enabled on your account, which leaves restricted and moderate content out of the results. When you are signed in, this feature can help ensure that your audience is not exposed to "adult content". Learn more about **SafeSearch.**

Report abuse: The Flickr staff works with the community to ensure an enjoyable experience for all. If you see something you feel violates the Terms of Service or the Community Guidelines, report it by doing the following:

Flagging a photo

1. Go to the photo's page.
2. At the bottom-right corner of the page, click Flag this photo.
3. Check the "I don't think this photo is flagged at the appropriate level" checkbox.
4. Click Submit.

The Flickr staff will review the photo in question.

If you come across content that you think might be illegal or prohibited, use the **Report Abuse system** instead.

Reporting abuse

1. At the bottom of any Flickr page under "Community," click **Report abuse**.
2. Select the issue from the pull-down menu.

For more information about Yahoo Flickr, visit **Yahoo Help**.