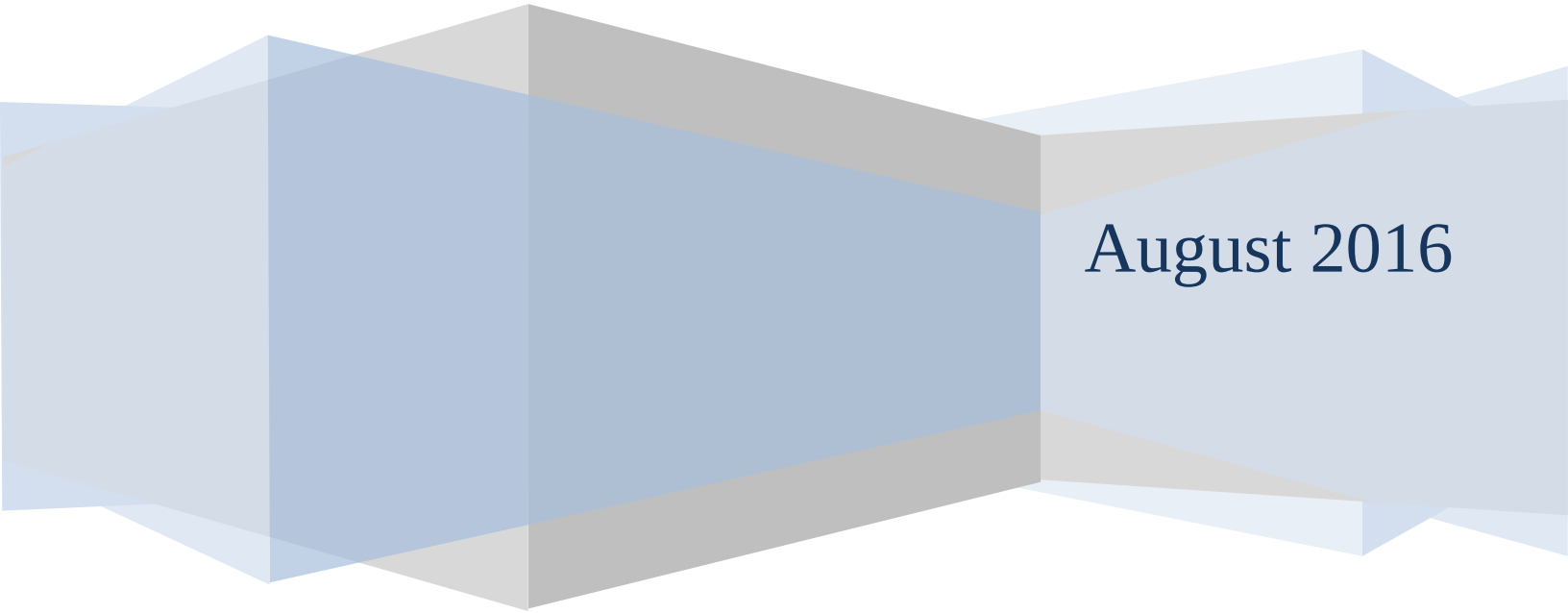

Cyber Security Awareness

For Social Media Users

August 2016

Contents

Disclaimer: This material and the information contained herein are intended to provide general information on cyber security. This material contains information sourced from official help forums/support pages of respective social media vendors (Facebook/Twitter/Google/YouTube/WhatsApp) and other social media security related information that is freely available online. DappsTech Private Limited is not rendering professional advice or services through this material. This material is completely free. We have assembled all those pieces of information that we consider as basics of cyber security and for detailed information proper links to their related vendor websites have been provided. Objective of this material is to spread awareness about cyber security, you can further use and redistribute this material for the same purpose. If you feel that any information provided here violates your copyright, please write to marketing@dappstech.com to have it taken down.

Social Media/Networking Security Best Practices

STRONG PASSWORD- A Strong password is hard to break and hack. Keeping a strong password for all online/social media accounts is a must. People tend to use a password that they can easily remember like mobile number, date of birth, birthplace, nickname, family member name etc. but it is not a good habit. These days all websites force their users to create a strong password but still due to carelessness/unawareness most of the people used to create a simple and easy password.

TIPS FOR STRONG PASSWORD:

1. A password should be 8-10 characters long.

2. It should be a mix of lower case, upper case, numbers and special symbols/characters like! " # $ % & ' ( ) *
+ , - . : ; < = > ? @ [
\ ] ^ _ ` { | } ~

Mix any of these in your password.

3. Do not use same password for each website.

4. Do not use a particular sequence like abcd/1234

5. Do not use common dictionary words.

6. Make sure that your backup password options (like recovery email/phone number) are up-to-date and secure.

LINKS- In social networking sites, people used to share different things with each other like media (image/video/songs), articles, and pages of different websites that contain the information of their interest. All kind of sharing on the internet happens through a link to that resource, this link is called URL or address of the web page. When a user clicks a link, it accesses that location through his/her browser, and if that location contains some malicious elements then the device (PC/Laptop/Smartphone) can get infected. However a good antivirus always shows a warning pop-up if you visit such links, but rather than relying completely on the warning messages from your antivirus software, it is better to avoid clicking

unfamiliar links, like a link embedded in the email that you receive from an unknown sender, offers and discount ads/pop-up messages, link from an unknown friend/follower on Facebook/Twitter/LinkedIn or in any other social media account, media file from an unknown friend on WhatsApp or other similar chatting apps etc. Always remember a properly formed URL/Address of website page always gives some hint about the type and location of the resource like the name of website/name of the page/name of the file if any of these is not clear to you then avoid clicking on that link.

These days in social media the **"Tiny URLs"** are in trend, these URLs give very little to no information about the website and this creates risk.

WHAT IS TINY URL AND HOW TO CHECK IT?

A Tiny URL is one which is shortened to hide the actual big URL/address of the website…a short URL does not reveal any information about the actual website and its resources, this feature makes it more attractive to hackers. Some social media websites like Twitter has a limit (Max Characters per tweet- 140, Max Characters per direct message- 10,000), this encourages users to share things with each other using shortened links but at the same time cyber criminals are using these links to share malicious things and redirecting people to phishing sites too…URL-shortening services such as TinyURL and Bit.ly are becoming popular attack vectors.

How to check Tiny URLs? You can use a URL expander that expands the URL and shows you where the URL is pointing to…some browser specific plug-ins are available, you can try:

URL EXPANDERS FOR CHROME -

https://chrome.google.com/webstore/search/url%20expander?hl=en

URL EXPANDERS FOR FIREFOX-

https://addons.mozilla.org/en-US/firefox/search/?q=longurl&cat=all

These expanders will show you a preview of the actual page before you click the link.

And if you don't know how to do this then do not click on any Tiny URL that you receive on social media.

MANAGE YOUR PRIVACY SETTINGS- Check your social media account's privacy settings and set these settings to the maximum secure level possible.

DON'T REVEAL PERSONAL INFORMATION- Do not share your personal information with anyone online like home address, DOB, Phone no, ID card number, Pan card number, mother's name or any other personal information that is generally needed for your identity.

If you are sharing images from the Smartphone- Turn off the location service. Because your images contain metadata and this metadata includes your location information if your location services are on.

Go to settings → locate location services → turn off (you can choose to turn it off only for camera as well)

DISABLE AUTO LOGIN- Do not set auto login for any app and social media account and do not select yes on 'remember login and password for this website' message that your browser displays.

CHANGE YOUR PASSWORDS FREQUENTLY- It's a good practice to change passwords of different email and social media accounts frequently. Set an interval for changing password like one month/three months/six months.

CLOSE OLD ACCOUNTS THAT YOU DON'T USE ANYMORE- You should close your old emails and other online accounts that you no longer require. This way you can minimize online sources that can provide your personal information.

Facebook Security Best Practices

1. For any social media account, the **strong password is a must**. Protect your password using the tips given in the "Social Media/Networking Security Best Practices" section. Don't use your facebook password anywhere else online. Do not share it with anyone.

2. **Do not click on the links** that are coming from some unknown source. In fact in the case of known source too, you should always think twice before clicking and downloading anything.

3. **Always log out your Facebook** account if you are using a computer that other people can use too, like in the office or public places. If you forget to log out your account, you can use remote log out feature.

4. **To log out of Facebook on another computer, phone or tablet:**

1. Go to your Security Settings
2. Click on the 'Where You're Logged In' section
3. Find the session you want to end and click 'End Activity'
4. Clicking End Activity will immediately log you off from the Facebook on that computer, phone or tablet.

5. **Log out your facebook account from Smartphone** in case you if you lost your phone to prevent someone else from accessing your account.

These are the steps:

1. Log into Facebook on a computer

2. Go to your mobile settings

3. Click Lost your phone? →Log Out on Phone

6. Check **"Where you're Logged In"** section of your Security Settings to see a list of devices and browsers that have been used to log in to your Facebook account recently. Each entry includes the date, time and approximate location when logging in, as well as the type of device used to access your account. If you are not able to recognize any of these locations then select that session and click End Activity.

7. **Login Alerts**- A very good feature, this notifies you whenever someone tries to log-in into your account from a new place/device. **To steps to turn this feature on are:**

1. Go to your Security Settings
2. Click the Login Alerts section
3. Choose the type of alert and click Save Changes

If you ever receive a login alert from an unfamiliar browser or location, follow the instructions in the notification email to reset your password and secure your account.

8. Understand and set your **Facebook Privacy Settings** carefully. Select the most secure options.

9. Do **think carefully before you post anything** on Facebook. Your status updates, photos, and comments can reveal more about you than you intended to disclose. Through your posts, anyone can track you, your location, your habits, your personality, your family etc. And this information helps cyber criminals to design targeted attacks for you.

10. Avoid participating in those survey/games/quizzes that take your personal information like **"25 Most Amazing Things About You",** avoid publicly answering such questionnaires and providing your personal details because such information is used to verify your identity.

11. Don't click on Tiny URL or short links; short links are those links that don't clearly show the link location. Sharing short links on Facebook is common but one should avoid clicking it. For more information read Tiny URLs section.

12. Beware of posts with suspicious subjects/ads like "Look at the video I found of you!" or any other similar kind, if you click the link on such post, you will get a message that there is a need to upgrade your video player in order to see this, and if you attempt to upgrade the video player, that page will instead install malware on your device, to track and steal your information.

13. Be suspicious of anything that sounds unusual like a friends request from foreign country, there are numbers of such fake profiles exist, from their profile pictures they look middle aged and mature, and they even sends a serious message that looks genuine but it is not!! Sometimes these fraudsters from overseas call you or give you a missed call using overseas numbers. If you do make a call back to these numbers, you will be charged Premium IDD (International direct dialing) rates.

--DO NOT call back to suspicious numbers especially IDD numbers.

-- DO NOT click on any fraudulent/suspicious hyperlink sent to you via SMS or email.

Sample of Scam numbers:

Numbers starting with +375, +371 , 081, +994, +670, +563, +382, +375, +371, +370, +261, +224, and +212

15. It is possible that your friend's account is sending out spam because their computer has a virus or bad software, or that their login info was phished. Here's what you can do to help:

--Report the spam

--Tell your friend to visit the Facebook Help Center to get help cleaning up and securing their account

How to avoid Scammers on Facebook?

Scammers on facebook create fake accounts or hack into existing Facebook accounts (sometimes of people you know). Then these scammers try to trick you into giving them money.

Here are some common scams to look out for:

Romance scams: Romance scammers typically send romantic messages, often pretending to be divorced, widowed or in a bad marriage. Their goal is to gain your trust, so the conversations may continue for weeks before they ask for money.

Lottery scams: Lottery scams are often carried out from accounts impersonating someone you know, or fake profiles pretending to represent an organization like Facebook. The messages will claim that you're among the winners of a lottery and that you can receive your money for a small advance fee. The scammer may ask you to provide personal information, such as your physical address or bank details.

Loan scams: Loan scammers send messages and leave posts offering instant loans at a low-interest rate for a small advance fee.

To protect yourself from scams, watch out for the following:

1. People asking you for money who you don't know in person
2. People asking you for advance fees to receive a loan, prize or other winnings
3. People asking you to move your conversation off Facebook (ex: a separate email address)
4. People claiming to be a friend or relative in an emergency
5. Messages or posts with poor spelling and grammatical mistakes

(Source: https://www.facebook.com/help/1674717642789671)

Also, set your profile settings to the maximum privacy/security possible, and before sharing anything on your timeline (especially on public posts) make sure that it does not reveal do much about you because scammers are hunting for such information and you are making yourself an easy target.

You can also use Extra Security Features provided by Facebook - https://www.facebook.com/help/413023562082171

Try General Facebook security tips:

https://www.facebook.com/help/379220725465972

(Source: Facebook help center resource/online informational articles)

Twitter Security Best Practices

1. For any social media account, a **strong password** is a must. Protect your password using the tips given in the "Social Media/Networking Security Best Practices" section. Don't use your twitter password anywhere else online. Do not share it with anyone.

2 If you connect to your twitter account on a public computer/shared computer, remember to log out before you leave.

3. Make sure that **you are on twitter.com**. There is a possibility that some third party websites or apps ask you to click a link for twiiter.com, but that link is not original, it is the address of some phishing website. This phishing website's login page often just looks like original Twitter's login page because they copy the whole look and feel. Make sure that address of this page is:

https://twitter.com

https://twitter.com/login

4. Use **login email alerts**, whenever you log in to your Twitter account from a new device/location for the first time, Twitter will send you a notification email. This extra security feature notifies you about any login attempt that is not done by you. If you receive such email and did not log in from the device mentioned in the notification email, you should follow the steps given in the same notification email to secure your account, starting by changing your Twitter password immediately.

Read more about this at https://support.twitter.com/articles/76036#new-login

5. Direct Messages (DM) are the most common medium to send malicious links on Twitter. Never open a message from an unknown sender and do not click any Tiny URL without verifying what it points to. (Either use URL expander extensions provided by your browser). For more information read Tiny URLs section.

URL Expanders for Chrome -
https://chrome.google.com/webstore/search/url%20expander?hl=en

URL Expanders for Firefox-

https://addons.mozilla.org/en-US/firefox/search/?q=longurl&cat=all

6. If your account has been compromised means someone has hacked your account but you are still able to log in, then use **the troubleshooting steps** provided by twitter's official help page- https://support.twitter.com/articles/31796

7. How to **check whether your twitter account has been hacked or infected?**

If you notice some unexpected behavior in your account like new followings are added, existing followers are getting removed/blocked, some unusual tweets have been posted from your account and some DMs have been sent to others from your account, if any such thing has happened without your knowledge…it means someone else is accessing your account and doing such things.

In this situation, the first thing you should do is to change your password. This will automatically log-off any other session on any other device. Then visit Apps in your settings. Delete any third-party app that you don't recognize.

You can also follow the instructions provided by twitter's official help- https://support.twitter.com/articles/31796

8. Twitter staff will never ask you to provide your password via email or direct message. **Do not click on any attachment, install software or update from an email that claims that it is from twitter's official team.**

9**. Unsafe links-** Sometimes Twitter gives a warning about the unsafe link which means the link or URL you are using or accessing is matching with some potentially harmful URLs stored in the Twitter's database. Whenever you encounter such harmful profile/tweets or URLs, report about that to Twitter team, **follow the steps given here**: https://support.twitter.com/articles/64986

To read more about unsafe links visit- https://support.twitter.com/articles/90491

10. **Fake Twitter emails**- Twitter will only send you emails from @twitter.com or @e.twitter.com. However, some users may receive fake or suspicious emails that look like they were sent by Twitter. These emails might include malicious attachments or links to spam or phishing websites. You need to remember that

Twitter will never send emails with attachments or request your Twitter password by email.

If you receive a fake email:

Delete the email from your inbox. Don't download any attachments from these emails.

Find out more about Twitter Safety at https://support.twitter.com/articles/76036

For additional security use Login Verification:
https://support.twitter.com/articles/20170388

Finally do not share or tweet any personal information on Twitter, Be suspicious of any communication that asks for your private contact information, personal information, or passwords. Think about how much information you provide in your Tweets, for more information about basic security rules that one should follow, read this - https://support.twitter.com/articles/18368

Google and YouTube Account Security Best Practices

1. To add an extra layer of security to your account, set up **Two-Step Verification**. For this:

1. Go to the 2-Step Verification page. You might have to sign into your Google Account. Visit- https://www.google.com/landing/2step/
2. Follow the step-by-step setup process.

Once you're finished, you'll be taken to the 2-Step Verification settings page. Review your settings and add backup phone numbers. The next time you sign in, you'll receive a text message with a verification code, now onwards Signing into your account will work slightly different, whenever you will login you will enter your password as usual but additionally you will be asked to enter the security code that is sent to your mobile via text, voice call or Google mobile app.

2. If you lost your device (laptop/phone) then the first thing you should do is→ revoke your app passwords and change your Google account password, this will prevent others from accessing your Google Account. App Passwords allows apps or devices that don't support 2-Step Verification codes to access your Google Account. If you use 2-Step Verification and accessed your Google Account from an app or device like Gmail on your iPhone or iPad, you probably used an App Password. Thus it is necessary to revoke app passwords if your device is lost or stolen.

Steps to revoke app passwords:

1. Visit your App Passwords page- https://security.google.com/settings/security/apppasswords
2. You'll see a list of the apps you've created App Passwords for. Click Revoke next to the application you no longer want to have access to your account.
3. Once revoked, that App Password can't be used to access your Google Account again. If you want to start using your account on an app or device again, you'll need to generate a new App Password.

3. **For Extra security use Security Key for Two-Step Verification**- After enabling Two-Step verification you can sign in your account only after providing two things- your password and your verification code (that Google will text you on each sign in) but these days some sophisticated attackers could set up lookalike sites that ask you to provide your verification codes to them, instead of Google. Security Key is a better option for such case but there are some limitations like your device should have USB port and you are using a chrome browser.

For more information read official information provided by Google: https://support.google.com/accounts/answer/6103523

4. Besides this always avoid clicking on short links or tiny URLs unless you know where this link will lead you to…means you should know the location it is pointing to. For more information read Tiny URLs section.

5. **It is good to follow general security best practices like:**

- Set a strong password for each online account, read about setting strong password at "Social Media/Networking Security Best Practices" section.
- Use a unique password for Google account.
- Change your Google account password frequently.
- Do not share any of your personal/financial and online account related information with anyone on mail/message/phone.

Additionally it is good if **you register a recovery phone number or email address** with Google. Follow the instructions provided here: https://support.google.com/accounts/answer/183723?hl=en

WhatsApp Security Best Practices

1. Anyone with your number can access your WhatsApp profile photo on his/her phone. To hide WhatsApp profile image the steps are:

1. Go to WhatsApp then Settings
2. Tap Accounts
3. Then Privacy
4. Tap Profile Photo and select ‘Nobody’

If you want to hide your profile picture/status and last seen from a particular contact, then:

1. Remove that contact from your phonebook.
2. Go to WhatsApp then Settings
3. Tap Accounts
4. Then Privacy
5. Set Profile Photo/Status/Last Seen to ‘My Contacts’

2. Never open a message from an unknown sender, do not accept unknown group invitations and **avoid clicking on any link and downloading** any kind of media unless you are sure that it is coming from a trusted contact.

3. **Beware of scammers**, like any other communication and social networking medium WhatsApp is vulnerable to online scams. Anyone offering a free subscription, claiming to be from WhatsApp or encouraging you to follow links in order to safeguard your account is definitely a scam and should not be trusted. These links could lead to those websites that install malware/spyware on you mobile to steal your personal and financial information. WhatsApp team will never ask you about your personal information and bank account details. Any mail from WhatsApp will come to you only if you have contacted their help team for support.

4. Be careful of what you chatting/sharing and with whom you are chatting and sharing your personal information. If some unknown person tries to chat with you, block that person.

5. Do not download any media file shared by groups unless you are sure it is coming from a secure source.

6. Hide WhatsApp images from Gallery/Photos

Photos exchanged on WhatsApp get automatically saved in a folder on your Smartphone's memory: internal storage or, SD card. And anyone who goes to your Gallery/Photos app can view them. Check out the following steps if you want to hide your WhatsApp images (these steps are for Android users, on other OS the steps can slightly vary):

1. Download a file manager app such as ES File Manager or, Cabinet Beta
2. Navigate to WhatsApp/Media/WhatsApp Images directory on the phone
3. Create a new file name .nomedia and save it

After this your WhatsApp images will not show up anymore in your Gallery/Photos app.

7. For Extra Security you can lock your WhatsApp. For this, you can use third-party apps as no such feature yet exists in WhatsApp. If you are using an Android phone, you can lock WhatsApp with FingerSecurity or, any other locking app available in the Google Play Store such as AppLock, LOCX.

For more information you can also explore how WhatsApp encryption works, visit: https://www.whatsapp.com/security/

You can also get answers to other questions related with WhatsApp functionality and security using official help section:

Steps:

1. Go to WhatsApp then Settings
2. Tap About and help
3. Then FAQ- This will take you to the online help FAQ (Frequently Asked Questions)section

About DappsTech

DappsTech is a technology company that is born out of an understanding that there is a growing need for Cyber Security awareness and services. At DappsTech we believe that Cyber Security aware society is the need of the hour. An educated and aware user can help in minimizing the impact and rate of cyber crimes, particularly of those that are related to online transactions and phishing…

http://dappstech.com/about/

Connect with us:

DappsTech YouTube Channel

DappsTech Twitter

DappsTech Facebook

DappsTech LinkedIn

DappsTech Google+