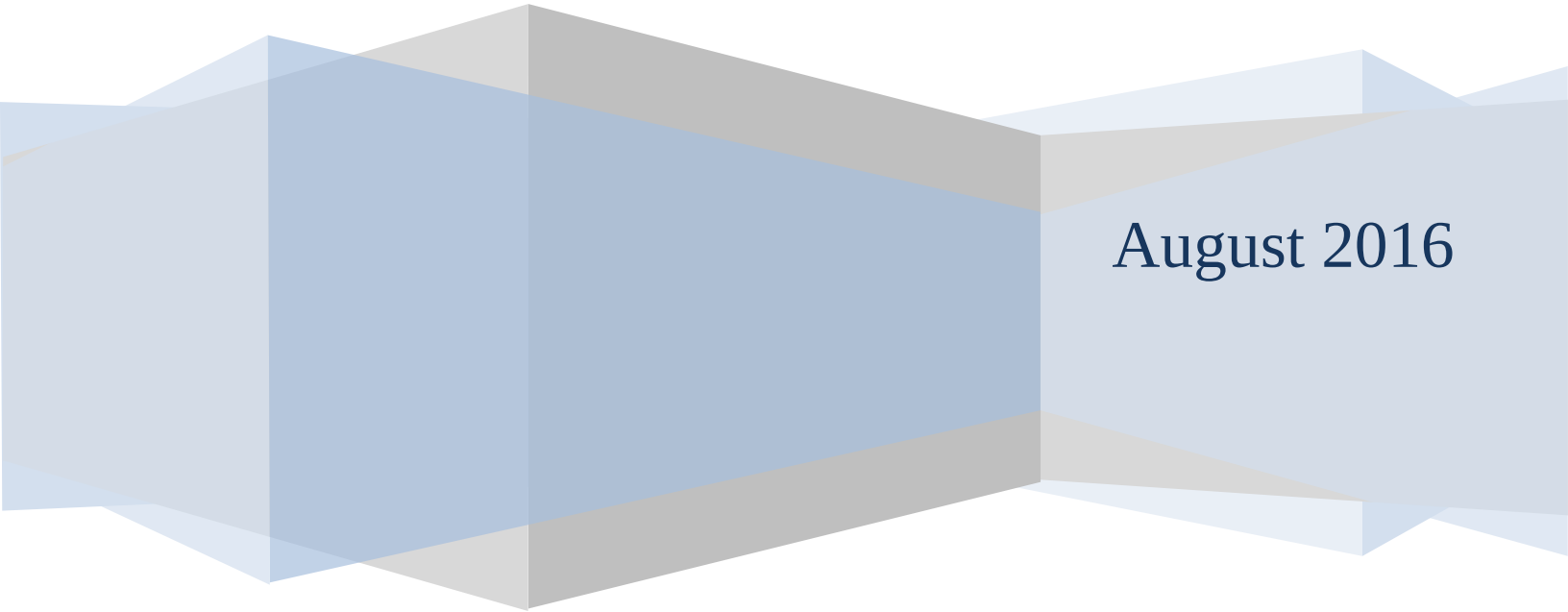

Cyber Security Awareness

Basics for non-technical 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 products vendors (Microsoft/Apple/Android) and other 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. The 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.

General Security Terms/Vocabulary

Over the last few years, the numbers of nontechnical users on the internet have increased, to target these nontechnical users cyber criminals are designing more and more sophisticated strategies because due to lack of awareness their chances of falling into such traps are high. This section covers the basics of cyber security that a person without any technical background should know, understand and follow.

Secure or 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 website forces the user to create a strong password but still due to carelessness/unawareness still 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.

7. Use a unique password for each of your online accounts.

Two-Factor Authentication or Two Steps Verification

When you enable 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account. You sign in with something you know (your password) and something you have (a code sent to your phone).

As per RBI guidelines, Two-factor authentication is must for all online credit card transactions in India

Suspicious Activity

Any activity that changes the normal behavior of your device…an alien/strange element on your phone like an unknown icon, file, image, message anything…You should be aware of what suspicious things/activities are causing trouble in your device.

Computer Virus

A computer virus is a software program that spreads from one computer (or Smartphone) to another and affects the normal operation of the computer. It may corrupt or delete your data and in the worst case may even delete everything on the hard disk.

Cyber Criminal

Cyber criminal is a person or group who try to steal precious information and money from the users of the internet.

Besides stealing critical information like credit/debit card number/pin/CVV and personal information like DOB/Address/emails/passwords etc. they try to track and spy on people and in some cases try to make them a target of something serious/harmful.

Social Engineering Attack

Social engineering in the context of information security is a kind of confidence trick for the purpose of stealing information and conducting fraud. The term "social engineering" is related to social sciences, it is considered as an act of psychological manipulation but in the context of the internet, it is used for cyber crimes. The most common purpose of social engineering attacks is to steal confidential

information from the users through fake calls on the phone, fake emails, fake links, and fake posts on Facebook etc. An example of social engineering attack would be that the cyber criminal contacts the target on a social networking site and starts a conversation with the target. Slowly and gradually, he/she gains the trust of the target and then accesses his/her sensitive information like password or bank account details.

SPAM

Spam is an irrelevant or unwanted message sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc. Spam is usually considered to be junk email.

RANSOMWARE and SCAREWARE

RANSOMWARE

Ransomware attacks are the latest in cyber attacks on web scams. Ransomware is malicious software that blocks access to a computer system and asks for money to unblock it. It's a denial-of-access attack that prevents computer users from accessing files.

How it works?

If you click on an infected popup advertisement or you visit an infected website, the hackers take control of your system, put it on hostage and attempt to extort payment.

How to protect yourself from RANSOMWARE:

1. Use antivirus and firewall from a trusted brand.

2. Keep the backup of your data, either in some external hard drive or online backup service. Backup your data regularly.

3. Turn your pop-up blocker on, avoid even accidently clicking on an infected pop-up, and do not click any button on popup even if it says 'close' because these buttons are programmed by criminals.

4. Do not click on the links embedded in Emails/Facebook messages/Tweets or anywhere else unless you are sure that it is coming from a trusted source. Avoid suspicious websites.

5. If your system comes under such attack→ disconnect from the internet, simply shut down your system and start with a fresh install or take it to an authorized vendor.

SCAREWARE

Scareware is one of the popular social engineering tricks that make a user download malicious software, it causes shock, anxiety, or the perception of a threat in order to influence users into buying malicious/unwanted software/app. Through some visual tricks cyber criminals make users believe that a virus has infected their computer or Smartphone and then they suggest them to download fake antivirus software to remove it. Usually, the virus is entirely fictional and the software is non-functional or malware itself. Scareware formats include malware, adware, spyware, trojans, and viruses.

How to protect yourself from a Scareware?

Make sure you have a good and updated antivirus software installed.

Avoid visiting the unsafe website and clicking unrecognizable links.

When any such popup or message box appear on your screen, do not get panic and do the following

-Disconnect the internet

-Shut down the system

-Restart system and run antivirus scan, if Scareware program has disabled your antivirus software then reinstall it and then run the full system scan.

PHISHING and SPEAR PHISHING

PHISHING

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons through electronic mediums like emails, links, websites, social media posts/tweets, phone call etc. Phishing is one of the social engineering tricks that are used to mislead users. Phishing is a continual threat, and the risk is even larger in social media such as Facebook, Twitter, Google+ and WhatsApp. Phishing takes advantage of the unawareness and carelessness due to which a user is not able to recognize that the website he/she is using is not real.

SPEAR PHISHING

It's a more advanced and sophisticated form of phishing that is designed to target high profile users. Spear phishing is an email that appears to be from an individual or business that you know, but it isn't, it is from some cyber criminal who wants your credit card and bank account numbers, passwords, and the financial information on your PC. What makes spear phishing different from phishing is the research done by attackers on a target. In spear-phishing cyber criminals do not use the standard phishing email structure because their targets are high profile users, individuals or companies; they do extensive research on their targets before sending them an email. The nature of such attack is analogous to Spear fishing, an ancient method of spearing fish from rivers and streams using sharpened sticks.

How to protect yourself from PHISHING or SPEAR PHISHING?

Awareness and caution can protect you from phishing/spear phishing kind of attacks. Always remember that a genuine person or organization will never ask your sensitive information via email.

Never submit confidential information via forms embedded within emails.

Do not get pressured into giving sensitive information or money to such cyber criminals, always report the support team of the respective website first and if it is serious then take proper legal action.

Do not click any button of an unfamiliar popup window and do not click any link unless you are confirmed about its authenticity.

Enter your username and password only when there is “https” prefix in the URL, it indicates that the connection is secured.

Sometimes emails and websites look just the same as real ones. But they are not; it is some malicious website that looks like the real one. Read the address of the website carefully because there will be some differences or mistakes in the spelling…before using a website first ensure that you are on a right website.

If you can, don’t log into online banks and similar services via public Wi-Fi networks in airports/metros/railway stations/cafes or on the streets.

Check the email address and website address carefully, if something is looking wrong then it probably is wrong…

Do not share any sensitive/personal information on the phone too…

LINKS, MEDIA FILES, and ATTACHMENTS

Do not click any link or download any attachment unless you are sure that is coming from a trusted source, no matter from where it is coming to you through SMS/WhatsApp message/Facebook post/tweet or email.

A valid URL will always include:

name_of_the_website.domain_name/name_of_the_file

Here ‘name_of_the_website’ is important, if the name of the website is not familiar to you, then you should avoid clicking it before checking its validity.

How to check whether the website you are visiting is safe or not?

Go to Google.com and search name of the website only; there would be some information about its authenticity. If you are not able to understand and to find any relevant information in this way then you can try online website security checkers like:

GOOGLE SAFE BROWSING
https://www.google.com/transparencyreport/safebrowsing/diagnostic/?hl=en

PHISH TANK

https://www.phishtank.com/

WEB OF TRUST (WOT)

https://www.mywot.com/

Protect Your Devices (PC/Laptop/Smartphone)

Some routine practices that can help you to keep your device safe

Install good quality anti-virus software, it is worth to spend some money to protect your device.

Keep your antivirus software updated. Set auto update…

Perform scans frequently; set an interval like weekly/ monthly.

Don't click on email links or attachments, unless you are sure about it. Avoid downloading media from untrusted websites.

Take the backup of your system regularly, so that in case your device gets infected you can easily reinstall a fresh Operating System and in the case of Smartphone, reset the mobile.

Surf smartly; be suspicious of malicious websites…

What are the symptoms that my device has been infected?

Your device (PC/Laptop/Smartphone) behaves in a strange way, it works or looks different than normal.

You see some unexpected icons/images or messages on desktop/home screen.

You hear unusual sounds and some of your programs start unexpectedly.

Your system Hang or Freezes frequently and when you try to open something it runs unusually slow.

Lots of system error messages get display on your screen one after the other.

The operating system will not load when you start.

You notice that some files or folders have been deleted or changed.

The web browser gets hang and does not allow you to close a browser window.

Note: If you notice any of the above, it is not necessary that it is due to some virus, there may be some hardware or software issue. So don't get panic!

Follow these steps:

1. Disconnect the internet from your device.

3. Shut down the device immediately.

2. Restart again, if your Operating System does not load, start your device in Safe Mode → for computer/laptop you need to press and hold F8 key till it starts in Safe Mode, for Smartphone steps are vary for each device follow the instruction given in the help/manual to open your Smartphone in SafeMode.

3. Run a full system scan for your device.

4. If a malicious program found follow the guidelines provided by your anti-virus software to disinfect or delete it.

5. Take the backup of important files and reinstall OS, in the case of Smartphone → Do a factory reset to set your phone to default settings. (This step will erase all information stored on your device)

To detect a virus on your computer manually:

A. Run antivirus scan

B. Generally, viruses like to hide inside your "Temp" folder so check it manually from there:

1. Close all the open windows/files… (because any opened window/file will have an associated Temp file)
2. Go to Start- Then type Run- in run box type %temp%
3. Remove all the files available…in some window OS except one system file all other files will get deleted.
4. Inside the Temp folder →Right click the mouse and click refresh if new files get generated again and on each click numbers of files are increasing; it indicates that your machine is infected.

Some Extra Inputs:

Every internet user should know some basics of internet and security as you spend a good amount of time on the internet. Be aware because somewhere someone is keeping an eye on you and your activities.

Make sure that you are using the trusted website and if you found something different on your regular website page, like a new box or button on the login page of your bank account, then confirm with the bank about that change first and then proceed.

Your social media account is your private asset that is stored in a public storage called the internet, its id and password is the lock and key to this storage. Do you want you lock and key to be strong or weak? The choice is yours…in the age of internet and technology private information is as precious as money. No app is designed to undo the mistakes made by humans…so the best approach is to be aware.

Lastly, if you do not have time to Google and explore about the status of a particular app, then follow a golden rule…do not install any new app on your Smartphone, instead use the apps that are already (by default) installed on your phone…these days each vendor sells mobile with some pre-installed popular utility apps….these apps are enough for a normal non-technical person. By allowing your kids to install whatever they want you are putting yourself at risk…most of the malicious apps come in the form of games for kids. Simply uninstalling a malicious app or game from the phone does not solve the problem. If your antivirus has detected some problem in your Smartphone then it is better to reboot the device, by resetting it to default…as we do with our laptops and PCs.

Each product vendor provides a dedicated 24/7 team to support its users from any kind of security attack. For official help and support visit the website of your device vendor, you can try some of these links:

Microsoft Support- https://support.microsoft.com/en-in

https://www.microsoft.com/en-us/security/default.aspx

https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses

Apple Support- https://support.apple.com/en-in

https://support.apple.com/en-in/HT204169

https://www.apple.com/in/support/security/

https://support.apple.com/iphone

https://support.apple.com/en-in/mac

How to avoid or remove Mac Defender malware in Mac OS X v10.6 or earlier: https://support.apple.com/en-in/HT202225

Android Support- http://www.androidcentral.com/help-my-android-has-malware

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+