CHAPTER

Online Security 11

INFORMATION IN THIS CHAPTER

- Security
- Online security
- Common online threats
- Identify threats
- Safety precautions

INTRODUCTION

In the previous chapters we have fiddled a lot with the internet. We have used a variety of tools to access it in different forms, we have also been to some of the lesser touched areas of it and also learned about how to stay anonymous while doing so. We also learned about some tools which would help us during the analysis of all the data we have collected from this massive information source. In this chapter we are going to touch upon a topic which has become very relevant in today's digital age and it is online security. Internet is a great place where we can learn different things, share it with others and much more. Today internet is available worldwide, and accessing it is pretty easy. We have devices which allow us to stay connected even on the move.

Today we rely on the internet for our many needs such as shopping, paying our bills, registering for an event, or simply stay social. Even our businesses rely on the internet for their day to day operations. We as a user of internet use different platforms, click on various buttons, visit various links on a daily basis. For an average user, it may seem pretty simple but involves huge amount of technical implementation at the backend.

Similar to our physical world this virtual world also has security issues. It's no big news that daily people are becoming victim of cyber-crimes. There are a variety of threats which we face in this digital world and sometimes we don't even recognize them. For example, we all get that spam message stating that we have won a huge amount of money in some lottery and we need to share some details to receive it. Although most of us simply ignore such messages, some people do respond and are victimized. Similarly we have already seen how the information we share online might reveal something about us that we don't intend to. This kind of information in wrong hands can be used against us. Recently there have been many cases which involved hackers attacking an employee's machine to gain access to the corporate data. The

Hacking Web Intelligence. http://dx.doi.org/10.1016/B978-0-12-801867-5.00011-2

main reason behind the success of such attacks is the lack of security awareness among the users. Though understanding the technical aspects of cyber security can become a bit complex for a nontechnical person but understanding how some of the common attacks work, learning how to identify them, and finally how to mitigate them is a necessity for every user. One question that is mostly asked by people is that why would someone try to hack us though we don't have any sensitive/financial information on our computers. Instead of answering this question right away let's learn about some of the attack methods and then discuss why someone would attack an average user.

We are in a world where we love to spend more time online than in social. The reason may be anything starting from shopping, e-mails, social online hangout, chats, messages, or online recharge or banking. We may use internet for our professional use such as it may be part of our day to day job or for personal use to browse or surf. Anyways the motive behind discussing is that internet is now an integral part of life, and it's quite difficult to avoid it.

Earlier we came across about only one aspect that is internet privacy: how to maintain privacy using different online solutions, browser setting, or anonymity applications. What about the other aspect that we missed. That is security. So we need to also put some light on the security aspects of the internet.

When we say security aspect it's not just about using secure applications or visiting secure sites, or having security implementation on our system such as updated antivirus and firewall. In this case security also means about data security or to be precise internet data security.

Securing not only the data of an organization will make it secure but also the users' data that's also quite important. So in case of data security we need to focus on both organizational data as well as users' data. For example, let's say an organization implements proper security mechanism to secure its data. All kinds of security softwares starting from antivirus, firewall, intrusion detection system, intrusion prevention system, and all other security tools implemented or installed in a system but if the security question of the HR's (Human Resource) e-mail id is what is your favorite color and the answer is pink then all these security implementations will go vain. So it's both the users' data as well as organizational data that are important and we need to take care of both.

As an organization we discussed a little bit on how the metadata can disclose certain information and how DLP (data leakage/loss prevention) can be helpful to secure all those. But from a user perspective it is also quite important not to share details in public that can be used against us or our security, for simple example, do not disclose information in public that can be used to know more about our way of thinking or about our certain area of interests. Let's say we disclose information that can be used to recover our password such as the answers related to any security questions, e.g., who is our favorite teacher, what place we like the most, what is mother's maiden name etc. These are common security questions which we generally find in different online applications that can be used as an additional verification to recover passwords. If we will disclose these information in public, let's say in any social networking site, blog, or anywhere else, that can be a threat to

our security. So think twice before disclosing any such information in the internet. The other way around is to select a wrong answer to such security questions. For example, for the question what is your favorite color, if we provide an answer such as pit bull, it will be quite difficult for someone to guess this answer and recover your account. Password reset is one of the examples for such an act, there are many other ways where information provided by us can be used against us such as social engineering attack, simple phishing attack, etc. Let's take another example such as if we tag ourselves in a particular place in a particular date most of the time then our present can be expected there and any ill-minded person can use it to exploit us. Other example can be if we show a particular hardware information or show off about a latest gadget then also that can be used against us. For example, if we disclose that we use iPhone and that too a jailbroken then there are certain jailbroken iPhone-related vulnerabilities that can be used against us such as the default openSSH credentials alpine/alpine. An attacker just has to be in the same wireless network where we use our jailbroken iPhone and he just needs to guess the IP address to start an SSH connection and we know that the default credentials can be used there to compromise our device. It's quite common now a days and people getting hacked everyday for these silly mistakes or unintentional information leakage. The only way to secure online user data is most of the time awareness. Be aware and avoid such information leakage and surf safely.

It's not any certain type of information we provide that can be used against us. The information can be anything. So it's better to avoid disclosing any specific information in public internet. And precaution is better than cure so share your data accordingly.

If we are in the security field then we must know the importance of information gathering. There is a great saying that "if you want to win a battle then you should know your enemy first." The more information we get about a person or organization the more way we can find weakness in them and later that can be exploited. Now we will discuss the common threats and their exploitation.

MALWARES

Malware is a word which came from the combination of two words, malicious and software. The simple definition that can be derived from this is that any software that performs malicious activity can be considered as malware. There are different types of malwares based on their behavior. Different malwares have different functionalities and different modes of spreading the infection. If we think of infecting a targeted audience or person then collecting information related to him/her can help a lot. If we know our victim personally then we can provide him/her software of his/her interest infected with malware directly in any storage device or by sending him/her a download link remotely. If we need to execute it first time, then collecting information about the operating system and security implementation on that will help a lot. So as a user if we get any link from a known person or any stranger, do not install it directly. Think twice before installation or else you can be a victim of malware. Most of the malwares

come from online where we try to access certain restricted sites such as adult sites, free music, or software hosting sites etc. So as a user, verify the source before downloading anything. There are various classifications of malware, some of which are defined below.

VIRUS

Virus or Vital Information Resources Under Seize is a term taken from the normal virus that affects person and can be the reason for different diseases. Similarly the computer virus is a malicious code that when executes in a system, infects the system and performs malicious activity like deleting data, memory corruption, adding random temporal data etc. The only weakness of the virus is, it needs a trigger for execution. If our system contains a malicious software that is affected by virus until and unless we install that in our system there is nothing to fear. To avoid a virus infection use genuine updated antivirus.

TROJAN

Trojan is quite interesting malware, it generally comes as a gift such as if we visit restricted sites then we will get some advertisements such as we won an iPhone, click here to apply and all, or in popular paid games as free, then once user is lured to that and installs that after downloading then the application will create a backdoor and provide all user actions to the attacker. So to spread a Trojan, if the attacker will choose a popular demanding paid app, game, movie or song then the chances of getting more people are quite a lot.

Trojans are nonself-replicating but hide behind another program. It is recommended that do not install any paid thing that comes as free. You never know what is hidden inside that application and also use antimalware in system for better safety.

RANSOMWARE

As the name suggests, it is quite interesting malware which after infecting the system blocks some popular and important resources of our computer system and then demand ransom money to give back the access. Usually ransomwares use encryption technologies to hold our data as captive. The recommendation will be the same as mentioned above.

KEYLOGGER

Keylogger is a piece of malware that collects all the keystrokes and sends the same to the attacker. So when user inserts any credential for any site, the credential can be recorded and sent back to the attacker and that can be later used by the attacker for account takeover. The recommendation for this is if you are typing credentials for any transaction-related site or value-related to any critical information, always use on-screen keyboard.

PHISHING

It is one of the oldest and still popular attacks which are also used in many corporate attacks. It is a simple attack where attacker tricks the user by sending a fake link that contains a page that looks quite similar to the original site page that user needs to log in. Once user will login in that site the credentials will be sent to the attacker and user can be redirected to the genuine site. The major weakness in this attack is the site address. If a user will verify the site address properly then there is very less chance of getting a victim of phishing attack.

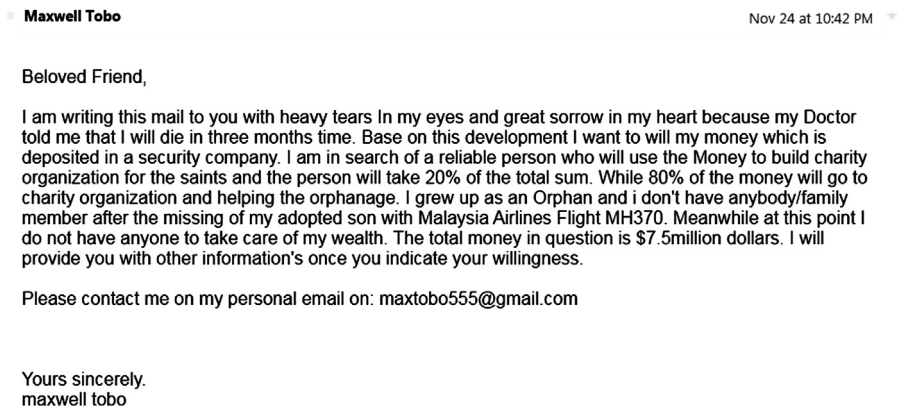
The information needed here is which site the target is having account on and which site the target generally visits quite often. So that later attacker can create a fake page of that and trick the user.

There are many new ways of phishing attack techniques available now. Some are desktop phishing where the host entry of the victim's system will be changed such as it will add an entry on the host file with the sites' original domain name with the address where the fake page is installed. So when a user types the IP address or domain name in the browser it will search for host entry. The host entry will redirect and call the fake page server, and the fake page will be loaded instead of the real page.

Another such popular phishing attack is tabnabbing. In tabnabbing when user opens a new tab the original page will be changed into fake page by URL redirection. There are also other popular phishing attacks such as spear phishing.

ONLINE SCAMS AND FRAUDS

One of the most widely faced issues online is the spam mails and scams. Most email user receives such mails on a daily basis. These mails usually attempt to trick users into sending their personal information and ultimately skim their money. Sometimes it is a huge lottery prize that we have won, or a relative in some foreign country who left us huge amount of money.



Maxwell Tobo Nov 24 at 10:42 PM

Beloved Friend,

I am writing this mail to you with heavy tears In my eyes and great sorrow in my heart because my Doctor told me that I will die in three months time. Base on this development I want to will my money which is deposited in a security company. I am in search of a reliable person who will use the Money to build charity organization for the saints and the person will take 20% of the total sum. While 80% of the money will go to charity organization and helping the orphanage. I grew up as an Orphan and i don't have anybody/family member after the missing of my adopted son with Malaysia Airlines Flight MH370. Meanwhile at this point I do not have anyone to take care of my wealth. The total money in question is $7.5million dollars. I will provide you with other information's once you indicate your willingness.

Please contact me on my personal email on: maxtobo555@gmail.com

Yours sincerely.
maxwell tobo

FIGURE 11.1

A sample spam mail.

Scammers also try to exploit human nature of kindness by writing stories that someone is stuck on a foreign land and needs our help and other such incidents. Sometimes attackers also pose as an authority figure asking for some critical information or as the e-mail service provider asking to reset the password. There are various Ponzi schemes which are used by scammers with ultimate purpose of taking away our hard earned cash.

HACKING ATTEMPTS

There are cases where we found that users with updated operating systems, antivirus, and firewall also face some issues and being victim of the hacking attack. The reason of those is certain popular application flaws that can be found in any operating system. Some such applications are Adobe Acrobat Reader or simply the web browsers. These kind of applications are targeted widely which covers almost all the operating systems and also widely used. So targeting these applications allows an attacker to hack as many as users possible. They either create browser plugins or addons that can help user to complete a process or to automate a process and the same in the backend can be used for malicious intention,i.e., collecting all the user's actions performed in the browser.

WEAK PASSWORD

Weak passwords always play a major role in any hack. For the ease of user, sometime applications do not enforce password complexity and as a result of that users use simple passwords such as password, password123, Password@123, 12345, god, own mobile number etc. Weak password does not always mean length and the characters used, it also means the guessability. Name@12345, it looks quite complex password but can be guessable. So do not use password related to name, place, or mobile number. Weak passwords can be guessable or attacker can bruteforce if the length of the password is very small, so try to use random strings with special characters. Though that can be hard to remember as a security point of view it's quite secure.

Strong password is also needed to be stored properly. Let's say, for example, I created a huge metal safe to store all my valuable things and put the key just on top of that. It won't provide security. It's not just about the safe but also about the security of the key. Similarly creating a very complex password won't serve the purpose if we write it and paste it on our desk which also should be kept safe.

SHOULDER SURFING

Shoulder surfing is always a challenge with a known attacker, a person whom you know and you work with. If he/she wants to hack your account then it is quite easy to do it while you are typing the password. The only way to make it difficult is that type

some correct password characters then write some wrong characters then remove the wrong characters and complete the password or else do not enter your password when someone around.

SOCIAL ENGINEERING

The first thing comes to our mind when we read social engineering is "there is no patch for human stupidity" or human is the weakest link in the security chain. This is a kind of attack which is done against the trust of the user. In this attack, first attacker wins the trust of the victim then collects all the information that is needed to execute one of the attacks we discussed above or any other attack. The only way to prevent from being a victim is trust no one, you never know when your boyfriend/girlfriend will hack your account. Jokes apart, do not disclose any information that has a possible significance with security to anyone.

So these were some of the security-related challenges that we face everyday, but we have only covered the problems. Let's move on to see what are the solutions.

ANTIVIRUS

As we discussed that there are various kinds of malwares out there and each one has unique attack method and goal. There is a huge variety of these and most of the computer users have faced this problem at least some point of time.

Antiviruses are one of the security products which are widely used by organizations as well as individuals. An antivirus is basically a software package which detects malwares present on our computer machines and tries to disinfect it. What antiviruses have is a signature and heuristics for malwares, and based upon these they identify the malicious code which could cause any digital harm. As the new malwares are identified, new signatures and heuristics are created and updated into the software to maintain the security from the new threat.

Many antiviruses have been infamous for slowing down the system and making it difficult to use, also the frequent updates have also annoyed people a lot. Recently antiviruses have also evolved and become less annoying and more efficient. Many solutions also provide additional features such as spam control and other online security solutions along with antivirus. The regular update is not just for the features but also to keep the database updated to maintain security. There are various choices in the market for antivirus solutions free as well as commercial, but it all comes down to which one is the most updated one because new malwares keep on surfacing everyday. One more thing that needs to be kept in mind is that there are also some malwares posing as antivirus solutions and hence we need to be very careful when making a choice for an antivirus solution and should download only from trusted sources.

IDENTIFY PHISHING/SCAMS

We encounter a huge number of scam and phishing mails on daily basis. Today e-mail services have evolved to automatically identify these and put them in the spam section, but still some of these manage to bypass. Here are some tips to identify these online frauds:

- Poor language and grammar: Usually the body of such mails is written in poor language and incorrect grammar.
- Incredibly long URL and strange domain: The URLs mentioned in such e-mails or the URLs of the phishing page can be checked by simply hovering the mouse over the link. Usually such URLs are very long and the actual domains are strange. This is used to hide the original domain and show the domain of the page that is being phished in the browser address bar.
- Poor arrangement of the page: The arrangement of the text and images is generally poor as many attackers use tools to create such e-mails, also sometimes the alignment changes because of the change in resolution.
- E-mail address: The original email should be checked to verify the sender.
- Missing HTTPS: If the page is usually an HTTPS one and is missing this time then this is an alarming sign.
- Request for personal/sensitive information: Usually no organization asks for personal or sensitive information over e-mail. In case such email is received it is better to verify by calling the organization before sending any such information.
- Suspicious attachments: Sometimes these kinds of e-mails also contain an attachment file in the name of form or document usually with strange extensions such as xyz.doc.exe to hide the original file type. Unless trusted and verified, these attachments should not be opened. In case the attachment needs to be opened it should be done in a controlled environment such as a virtual machine with no connection.

UPDATE OPERATING SYSTEM AND OTHER APPLICATIONS

One of the major methods used by attackers to gain access to our machines is to hack through the applications running on the system. The operating system we use or the applications running over it contain flaws in the form of vulnerabilities. Attackers use exploit codes to attack specific vulnerabilities and get a connection to computer systems. New vulnerabilities are discovered on regular basis and hence the risk keeps on increasing. On the other hand patches for these vulnerabilities are also released by the vendors. Keeping our machine's softwares updated is an effective method to minimize our risk of being attacked.

Almost all operating systems come with mechanisms which allow it to update with the recent patches available. They also allow us to manually check for updates and install if available. Apart from this other applications that we use such as multimedia players, document readers etc., also have patches and some of them are updated automatically while some need to be downloaded separately and installed.

Secunia PSI is a Windows-based application which helps us to identify outdated software and is also capable of automating the process of updating it. It can simply run in the background and identify the applications that need to be updated. User can download the appropriate patch and also install it. In case it is unable to do so it notifies the user and also provides useful instructions.

ADDONS FOR SECURITY

Web browsers are one of the most widely used applications on any platform and also the medium for most of the attacks. Let's learn about some easy-to-use addons which can help us to stay secure online.

WEB OF TRUST (WOT)

WOT is a service which reviews website reputation based upon crowdsourced method. Based on the review of the crowd the addon allows us to know how it is rated on the scale of trustworthiness and child safety. Similarly users can also rate a website and hence contribute to make the web a safer place. Details and comments about the website you are visiting can also be viewed which help users to make an informed decision. Using the applications is pretty simple, visit the website and click on the WOT addon in the browser bar and it will display the details related to it. The addon is available at https://www.mywot.com/en/download for different browsers.

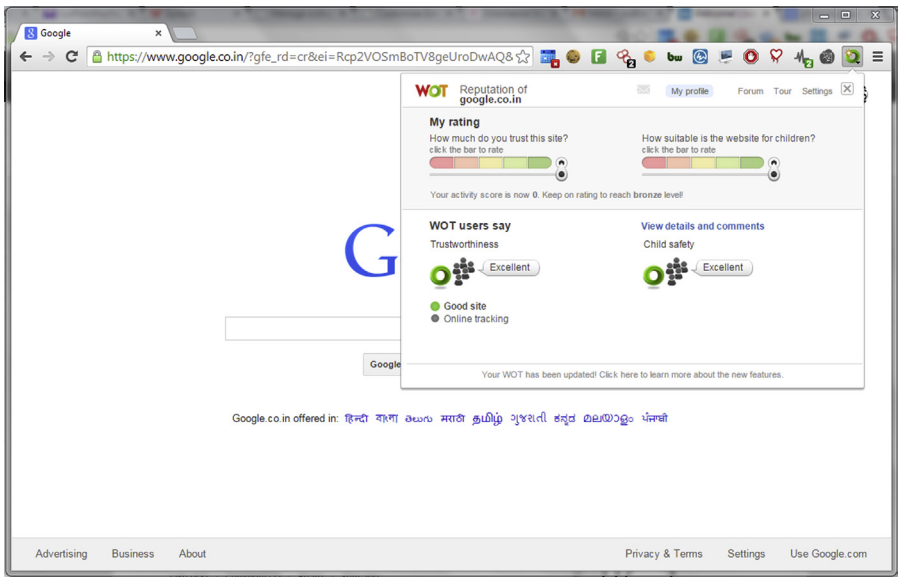


FIGURE 11.2

Web of trust (WOT) in action.

HTTPS EVERYWHERE

HTTPS Everywhere is yet another security-focused browser addon. Some websites have HTTP as well as HTTPS pages but don't use HTTPS by default or sometimes provide limited HTTPS support. HTTPS Everywhere allows to enforce the usage of HTTPS over such platforms and hence helps to make the data transmission more secure between the client and server. The addon is available at https://www.eff.org/HTTPS-EVERYWHERE.

NoScript

NoScript is a browser addon which allows us to manage the execution of JavaScript and similar active content technologies on websites. We can simply whitelist the applications we trust and block execution on others. This allows us to protect ourselves from Cross-site Scripting (XSS) and Clickjacking which are the most widely discovered and exploited web application vulnerabilities. NoScript is available for Firefox-based browsers and can be found at https://noscript.net/. The chrome alternative is ScriptSafe (https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf?hl=en).

TOOLS FOR SECURITY

Though not all of us have the technical understanding of running a full-fledged vulnerability scan and making a sense out of it, there are some simple tools available which allow us to perform a scan and identify the basic flaws in our machine.

For Windows-based machines we have Microsoft Baseline Security Analyzer (MBSA). MBSA is an application provided by Microsoft which helps us to test the baseline security of Windows and associated services. It basically looks out for missing software patches and common misconfigurations so that they can be patched. Apart from the base operating system it also checks for flaws in other Microsoft services and applications.

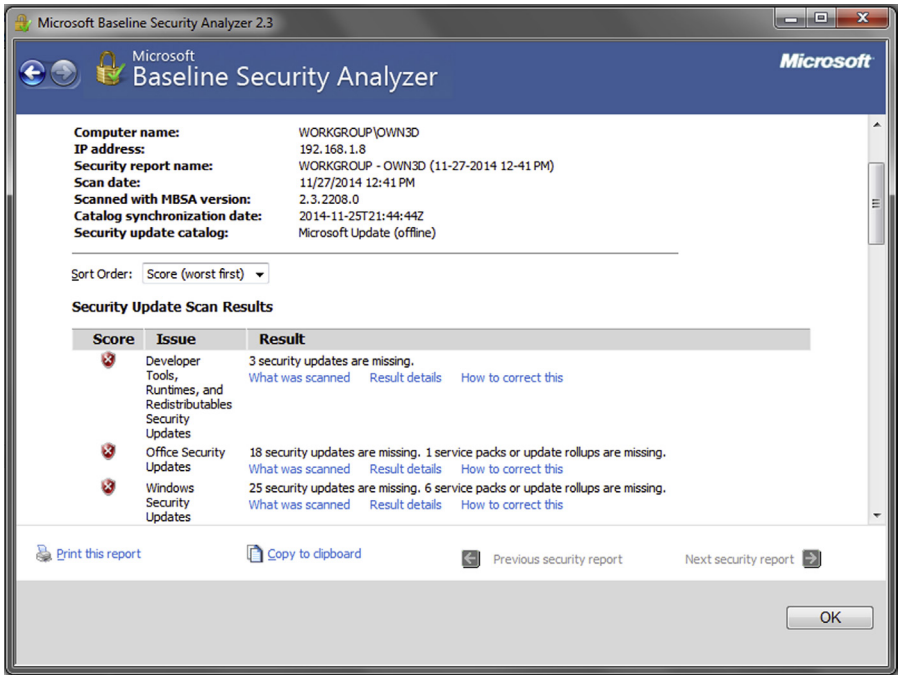


FIGURE 11.3

Microsoft Baseline Security Analyzer scan result.

Similarly there is Linux Basic Security Audit (LBSA). This is a script which aims at making the Linux-based systems more safe and secure, though the setting should be applied depending upon the requirements and might not be suitable for all scenarios. More details about it can be found at http://wiki.metawerx.net/wiki/LBSA.

Using such free and easy to use utilities we can certainly identify the gaps in our security and take appropriate steps to patch them.

PASSWORD POLICY

As we use keys to maintain the authentication in real world similarly we use passwords in the digital world. Passwords are combinations of characters from different sets of alphabets, digits, special characters which we provide to access and prove that we are the rightful owner of the specific data/service. Using passwords we access our computers, our social profiles, and even bank accounts. Though passwords are of such relevance most of us choose to have a weak password. The reason behind it is that as humans we have a tendency to choose things which are easy to remember. Attacker exploits this human weakness and try to access our valuable information through different techniques. Without going into the technical details of such attacks some of them

are guessing, trying our name, our parents/siblings/spouse name, our date of birth etc.; bruteforcing, trying every possible combination using automated tools/scripts; exploiting web application flaws such as SQL Injection. We cannot have control to mitigate all these issues yet we can make an effort to make our passwords strong enough so that they are not easy to be enumerate. General recommendations for passwords are that they should be at least 8 characters long, should contain characters(lower+upper case), digits, and special characters. This combination should be such that it cannot be easily guessed even people who know us. Sometimes people even create a weak password even after following these rules, one such example is "Pa$$w0rd." There are tools which allow attackers to generate a list of such combinations and use it to attack the user account. There is an online application which can be used to check the complexity of our password and tells us how much time will it take to crack it: https://howsecureismypassword.net/. Apart from this we should also not use that same password for different accounts because in case one account gets hacked it could also be further used to compromise our other accounts. This brings us to the problem of remembering many passwords, it can be solved by using a password manager such as LastPass (https://lastpass.com/). There are many other alternatives also available. Also choose your security questions wisely. We often forget what we have set as the security question and if someone asks us that question later we might reveal that information.

There are also various services which allow us to check whether any account associated with one of our e-mail addresses has been compromised. One such free service is HaveIBeenPwned (http://haveibeenpwned.com/) by Troy Hunt.

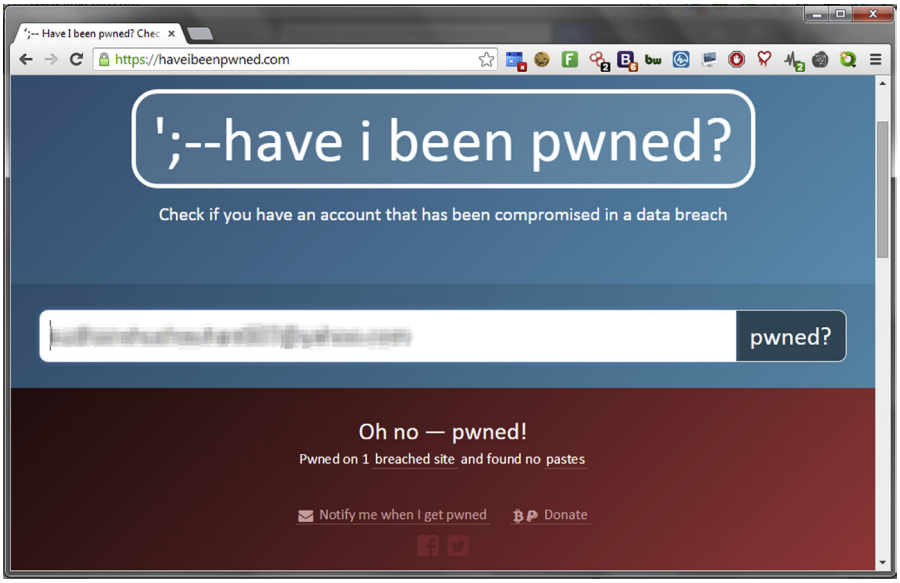


FIGURE 11.4

HaveIBeenPwned result.

PRECAUTIONS AGAINST SOCIAL ENGINEERING

One of the main techniques used by hackers to extract sensitive information from the victims is social engineering. We as humans are naturally inclined to help others, answer to authority, and reciprocate. Using these and other similar weaknesses (in context of security) of human nature, we are exploited by attacker to make us reveal something sensitive or take an action which might not be in our favor. People simply pose as the tech. guy and ask for the current password or tell that they are the CTO of the company speaking and ask the receptionist to forward some details. To safeguard against such attacks, security awareness is very important. People need to understand what information is sensitive in nature. For example, it might seem that there is no harm in telling someone the browser version we are using at the enterprise but this information is very crucial for an attacker. Also one may trust but must verify. People should ask for proof of identity and also cross-verify it to check if the person is actually who he/she is saying he/she is. In case of doubt it is better to ask someone higher in authority to make the decision than to simply do as told.

DATA ENCRYPTION

At the end the motive behind most of the attacks is to access data. One step to stop this from happening is to use a disk encryption software. What it does is that it will encrypt the specified files in our machine with a strong encryption method and make it password protected. In case even if the machine is compromised it would make it very difficult for the attacker to get the data. There are many such solutions available which provide this functionality such as BitLocker, TrueCrypt. It is advised to check if the software being used has no publicly known vulnerability in itself. Similarly it is advised to store and send all sensitive online data in encrypted format.

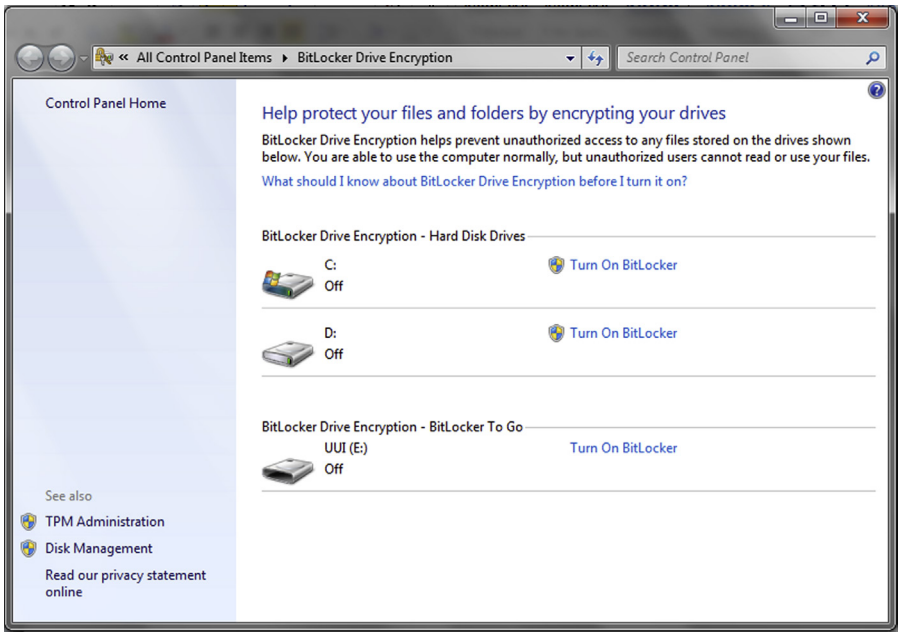


FIGURE 11.5

BitLocker Drive Encryption.

Some generic methods which would help us maintain our security online and keep our data safe:

- Don't open URLs that you don't trust.
- Try to understand what it means before clicking on "I accept."
- Don't download from untrusted sources.
- Don't ignore abnormal behavior (regular system restart, crash, hard disk filling up without any reason etc.).
- Backup important data on regular basis.

There are multiple motives behind such attacks and unlike popular beliefs they are not just targeted on big corporations. As already discussed most of the attacks being a spam mail or phishing are simply used to directly take the money of the victim, but some attacks have a bigger reason behind. Some of the attacks are made to extract information which could be leveraged to gain further confidential information, for example, attacking an employee's personal computer to extract information which could allow access into the corporate network. Similarly some attackers simply need to have a connection to victim machines so that they can use them later for different purposes such as Bitcoin mining, as a proxy to attack others, as part of a botnet for sale etc.

So we learned about some of the common methods used by the attackers and also how to identify them and safeguard from them. The virtual world is pretty insecure though there are various products and services out there which could help to minimize our risk none of which can guarantee security. Humans being the weakest link in the security chain are the easiest target for attackers. It is only by our awareness, understanding the attacker methods and taking right precautions which would make us digital life safer.