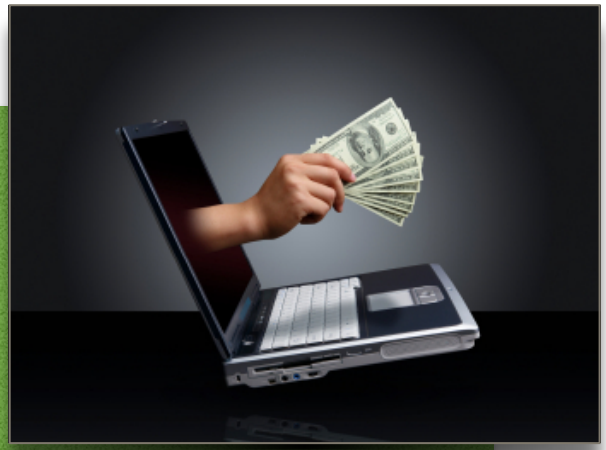
Banks and payments on the internet



Introduction

Do you think payments on the internet are safe?

We don't think that this is really safe nowadays. Have you ever considered that your password and credit card numbers are giving someone else access to your account because of phishing, pharming or viruses?

In 2015 you can do a lot of things on the internet for example shopping, communicating and payments. There are a lot of good aspects of the internet, but today we're going to talk about the bad sides of the internet in payments and banks.

For example there are people who use various methods to steal money. They want to take information from us.

Today you need to be careful with personal information and you can't trust every site. There are a lot of different ways someone can harm an internet user, such as through ads and viruses.

Some important words

Phishing- the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware.

Pharming- a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

Viruses- a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be ”infected".

Continuing

So, why is this a problem then? The first thing is that there are people who want to take your money. They can do it with a fake bank site or advertisements. So, the thing is that everyone is in constantly danger.

The second thing we've thought about is when you buy something online pay before the product is delivered. This is not actually a problem but when you've come to the wrong site and order a fake product it gets complicated. It's hard to find the fake seller when you've paid for it because they've a great talent to disappear in this phase.

Suggestions

The main way to prevent having someone guess a password is to have a password that has nothing or little to do with yourself. A combination of letters or words, numbers and special characters is the hardest to guess. If the user has some trouble remembering passwords, using a date or a name is the best solutions for them. However, even then there can be some added security. Strange capitalization and swapping letters for numbers are the easiest ways to make a password harder to guess.

The easiest way to prevent an incident of theft due to the use of a public computer or network is not to use either of the two to log in an Internet banking account.

However, not everyone has the option to use a private computer for banking. In that case, the user has to use Private Browsing. This mode leaves no traces of internet use. It basically looks like no one has used the browser. If the user has not used Private Browsing, their best option is to delete all the browsing data. This should have the same outcome as using a private mode on the browser.

There is not much to be done regarding the use of a public network. The only solution is to avoid it totally.

There are not many ways someone can prevent being phished. The best way is to be really careful when making any online purchases or checking a bank account balance. When visiting a website that requires you to enter any personal information, the user has to check various characteristics of the page in order to determine if it is legit or not.

One common practice fake websites use to deceive the user is using the exact same layout as the original website but with a small mistake in the link or other little mistakes that the user does not notice. In this case, the user has to check that the link and the site look exactly as they should. Another common way to deceive users is using ww,ww3 or other similar prefixes instead of www. In order to determine that the site is safe for transactions, the link prefix should be https:// and not http://.

Protection is the key to avoid getting infected by malware. The best solution is the use of an antivirus program, which will detect, block and clean the malicious software or files on a system. However, viruses are only one category of malware so antivirus programs may not detect other kinds of malware. This is the reason why people are often advised to use an antivirus program as well as having an anti-malware program installed but not running. This way there is a protection from viruses and a scan can be run using the anti-malware program to ensure that the antivirus has not overlooked something.

Links

If you want more information about this you can check this website called One Dollar Lesson. Here you can find great facts about internet security. There are more information when you scroll down.
http://onedollarlesson.com/

Naked Security is also a site where you can find 8 tips for safer online banking.
https://nakedsecurity.sophos.com/2013/10/03/8-tips-for-safer-online-banking/

Case 1:

Many people in Greece have received an email saying that they have inherited a sum of money from a deceased family member. They ask various sensitive information such as bank account or credit card information in order to confirm the identity of the person, who will then supposedly receive the amount of money mentioned in the email. Of course, this never happens and the person who sent the emails gains access to information that some victims have filled in and sent.

Case 2:

A friend had once purchased a designer jacket from an online store. After paying using a credit card, she waited for the product for a week but there was no sign of it. She tried to call the store but no one picked up. She emailed them but there was no response, so she called the police. They managed to find the owners of the store and get the money back and him in jail.

Case 3:

Yesterday I got an email from a "21 year old girl named Sandra". She said that she's from Ivory Coast and she needed my help. She said she was trying to escape from a political war after the loss of her mother and older brothers. Later her father got killed, and she was informed that she had inherited 9 million dollars since she was the last daughter alive. So she wanted to use my bank account in my country to transfer her inherited funds and asked for a letter of invitation that will allow her to get a visa to my country so that she can continue her education and invest the money in a viable business venture. She also said she was willing to give me 15% of the money.

Summary

To sum this up this presentation we would like to say that there are both good and bad sides of the internet. We've talked about problems with banks and payments on the internet. You've already heard this like a thousand times but we will say it once again: it's really important to create a strong password.

It's important to access your accounts from a secure location. You need to think about the link prefix. It's also necessary to use antivirus programs.

And one last thing: You don't have to be afraid of the internet, only aware of what could happen!

Cornelia,
Leonidas,
Aleksander,
Kamilla &
Hanna-Klara