After mid week one

Internet Security – Cookies

Cookies are files, generally from the visited WebPages, which are stored on a user's computer. They hold a small amount of data, specific to a particular client and website, and can be accessed either by the web server or the client computer which can be usernames, password, session token, etc.

Types of Cookies

There are three different types of cookies:

**Session Cookies:** These are mainly used by online shops and allows you to keep• items in your basket when shopping online. These cookies expire after a specific time or when the browser is closed. **Permanent Cookies:** These remain in operation, even when you have closed the• browser. They remember your login details and password so you don’t have to type them in every time you use the site. It is recommended that you delete these type of cookies after a specific time.

**Third-Party Cookies:** These are installed by third parties for collecting certain• information. For example: Google Maps.

**How to Block Cookies and Delete Them?**

**Internet Security – Phishing**

**How to Detect a Phishing Email?**

* Spelling and Bad Grammar
* Links in Email(security has been compromised)
* Spoofing Popular Websites or Companies
* Salutation

**Got Phished by Mistake?**

What to do in case you think that by mistake, you got phished? In such a case, you can take the following measures: Change the passwords immediately of the account that you think has been hacked.• Check if any money has been withdrawn or any payment done through your• account. You can contact your financial institution directly for this. Contact the authority on whose behalf you got that email. You should also report• to your account administrator.

**Internet Security – Social Network**

Social Networking is the use of Internet based on social media systems to get in touch with family, friends, customers, classmates, etc. Social Networking can be done for social purposes, business purposes or both. The programs show the associations between individuals and facilitate the acquisition of new contacts.

**Internet Security – Chrome**

**Internet Security – Mozilla**

**Internet Security - Internet Explorer**

**Internet Security – Gaming**

There are different types of online games:

* Single user playing game like Miniclip
* Multiple player games
* Cross-platform online game
* Real-time strategy game like Imperia
* Browser games which utilizes directly the Internet explorers

**Risks from Online Games**

Nowadays most of the online games are multiple user games and the risk that comes from other users are very high and are as shown below:

**Viruses** – The player can be attacked from email attachments, phishing or instant• messaging. This can result to the hacking of the user computer or the network.

**Malicious Software** – Attackers can use online games to redirect the genuine• users to a fake webpage to steal their credentials.

**Hacking that comes from Hacked Gaming Servers** – This hacking can come• when the server of the game has been compromised because of its vulnerability as a result this can put all the users in danger who are connected to this gaming server.

**Insecure Game Coding** – This is another type of known vulnerability where all• the data of users like name, surname, credit card information can be stolen because of an insufficient security on the programming code.

**Social Risks**

This risk comes from social interaction with other malicious users who want to steal your data which can be:

Your personal Information

Credit card details

They can pretend to be a child and contact other children asking them to reveal

other information.

Threats in Online Gaming

Threats at games are of different types and for different purposes which can be to gain unauthorized access to play the game generally. This technique is done by stealing others’ password.

A few other very often used techniques are:

Dictionary attack

• Social engineering

• Malware infection

• Corruption the genuine authentication software

• Phishing user ID and password by sending emails.

**Hackers can cheat at the game for the purpose of: Stealing virtual property**

• To obtain higher levels of plays

• Corrupting the gaming software which controls the levels of play

• Skipping the policies

• For making DoS to the gaming provider.

• Paying for the game by using Trojans to hack and steal the Card ID and otherdetails

What to do for secure online game playing?

Encrypt critical game data• Minimize client’s data• Create a security tutorial for the players• Complex password policy• Audit trails and logs• Patching bugs• Always use an antivirus software on your computer.• Be prudent when opening files and links sent by other users over instant• messaging of game. Validate authenticity of the new release of software’s.• Create complex passwords.• Update your computer. Connect securely with your browser.•

**Internet Security – Child Safety**

Social Rules Regarding Child Internet Safety

* The computer should be placed in the living room
* Discuss with your child
* Set time limits for Internet usage
* Never reveal personally identifiable information
* Don’t let your kids open attachments
* Use programs to save writing logs

**Use Software to Keep Track**

Here is a list of software that are helpful in keeping a track of what is being viewed on your computer.

* OpenDNS
* ContentWatch Net Nanny 7
* Qustodio Parental Control 2015

**Internet Security – Spamming**

Spam is a form of email which is used to send to different email accounts and in general contains advertising about any product or services. But the real problem is when they contain malwares that can damage the user’s data.

**Anti–Spamming Tools**

* Aevita
* Spam Experts
* Spameater
* SpamWeasel
* AntispamSniper
* Spam Reader
* MailWasher

**Internet Security – Chatting**

Chatting is a communication over the Internet that offers a real-time transmission of text messages from the sender to a receiver. Chat messages are generally short in order to enable other participants to respond quickly. Thereby, feeling similar to a spoken conversation, this tool is an attractive place for cyberattacks to hack account and get data.

**Risks from Chatting**

* Viruses
* Malicious software
* Hacking that comes from Hacked Chat Servers

**Internet Security – File Download**

Downloading can be for many reasons from entertaining like downloading songs, movies, clips also for information gaining like documents PDF, WORD, photos, etc. or for software updates.

**Internet Security – Transactions**

The transactions happen in the following forms:

When you go in a market and you use a POS for payment, then a transaction occurs.

In your mobile phone when you download an android app to order something like the eBay app.

When you pay something through an online payment service like paypal.com.

**Check if You are Doing a Secure Transaction?**

A simpler indication is recognizing the difference between a secure and insecure connection of which Https:// is a secured site, while Http:// is not secured.

**What Should You do as a System Administrator?**

**Internet Security – Banking**

E-banking is an electronic payment gateway which enables all the customers of a bank to do banking transactions through their computers without the need to go physically to the bank.

Normally to create an e-banking account the client has to go physically to the bank to be able to open it and authenticate it when it opens. A customer can link this account with their loans, current account and many other bank products.

**Internet Security – e-Commerce**

E-commerce is all about selling or buying goods and services from Internet and paying through this medium. This transaction happens between clients to business, B2B, client to client and as in between there is money transaction we should be cautious when using and also while setting up e-commerce sites.

Top e-Commerce Platforms

* Magento
* Shopify
* WooCommerce
* Bigcommerce

**Internet Security – Certificates**

Digital Certificates are a standard of security for establishing an encrypted link between a server and a client. Generally, between a mail server or a webserver, which protects data in transitions by encrypting them. A Digital Certificate is also a Digital ID or a passport which is issued by a Third Party Authority which verifies the identity of the server’s owner and not claiming a false identity.

**Components of a Digital Certificate**

All these following components can be found in the certificate details:

* Serial Number: Used to uniquely identify the certificate.
* Subject: The person, or entity identified.
* Signature Algorithm: The algorithm used to create the signature.
* Signature: The actual signature to verify that it came from the issuer.
* Issuer: The entity that verified the information and issued the certificate.
* Valid-From: The date the certificate is first valid from.
* Valid-To: The expiration date.
* Key-Usage: Purpose of the public key (For example: encipherment, signature, certificate signing...).
* Public Key: The public key.
* Thumbprint Algorithm: The algorithm used to hash the public key certificate.
* Thumbprint: The hash itself, used as an abbreviated form of the public key certificate.

**Internet Security – Identity Theft**

**What is Identity Theft?**

Identity theft is an action when someone steals your name, surname and other personal data and uses them to do something unlawful. Nowadays, this is a very sensitive issue because many people transmit their sensitive data over Internet and the big as well as small companies have to take their incentives for anti-fraud policies in the work place.

**How Does ID Thefts Take Place?**

There are quite a few ways in which people or hackers can steal your ID. Some of the most commonly used ways are as follows:

* Most of the skilled people in such activities rummage through trash looking for
* invoices, bills and other papers with your personal information. By stealing wallets which can contain your ID card, credit card, and other
* personal identification details, etc. Stealing expired applications for preapproved credit cards and fill them out with a
* different address. Take important documents such as birth certificates, passports, copies of tax
* returns and the likes during a burglary of your house. Steal the Social numbers and identities of children who are especially vulnerable
* because they don’t have credit histories and it may be many years before the theft is discovered. Steal personal information from a book or a newspaper article.
* Steal personal information of a relative or someone that he or she knows well,
* perhaps by being a frequent visitor to their home.
* Hack into a computer that contains your personal records and steal the data.
* “Shoulder surf” by watching from a nearby location as he or she punches in a mobile phone.
* By phishing methods mentioned in the upper section by requesting you in general• to fill a form with your data.

**What to do if you are a victim**

You can do the following things as soon as u get to know that you have been a victim of ID Theft.

* Immediately call the police to file a report with your local law enforcement agency.
* Document all your steps like keep all the correspondence and copies of the documents.
* Call your bank to cancel all your ATM and POS transactions.

**Internet Security – Cybercrime**

**Types of Cybercrime**

Following are some of the most prominent cybercrimes happening around the world.

* **Financial Cybercrime**
* DoS Attack or Cyber Extortion
* Cyberterrorism

**Credit card cloning**

Everyone tends to think of all the great things that get accomplished with new technology. Smartphones allow us to have small computers in the palm of our hand. Medical technologies have cured certain diseases. And automotive technologies have given us the power to create cars that run on electricity.

[](http://www.ifcs.org/wp-content/uploads/2012/09/atm-cardskimmer.jpg)

Beware of anything that looks out of ordinary at your ATM machine like this.

But there are downsides to advanced technologies, and one of these downsides is the power that it gives hackers. Hackers have been preying on unsuspecting individuals for a long time, but thanks to the recent onslaught of credit card cloning, hackers are now stealing identities easier than ever before.

**What is credit card cloning?**

Credit card cloning is an identity theft tactic that allows hackers to create a fake credit card by stealing the information off an individual’s actual card. For example, a person’s credit card information is placed onto another card-like object and used just like a credit card.

**How does credit card cloning occur?**

A hacker places a device known as a skimmer on a popular card reading location, such as on an ATM or on the credit card reader at a retail store or gas station. The magnetic strip of a person’s credit card is then read by the skimmer as it’s swiped, and the information held on that magnetic strip is then sent to the hacker’s computer. Although the text is a jumbled mess of letters, numbers and symbols, it’s the right information needed to create a clone of the real card.

This information can then be transferred to another card with a magnetic strip, such as a hotel key, gift card or old credit or debit card. When this card is now swiped, it will act like the credit card of the victim.

**What makes cloning so unique?**

When most hackers receive your credit card number, they only receive the number. This means that they can really only make purchases and use your credit card online. Shopping online requires the hackers to have items shipped to them, making it much easier for them to get caught. Plus, a recent slew of online purchases will serve as a red flag to your financial institution, giving the hacker less time to enjoy their shopping spree.

On the other hand, cloning allows hackers to create a physical replica of your card, allowing them to go to restaurants or retail stores and use the card to make purchases. This gives them the ability to receive goods or services in real time and reduces their chances of ever being caught.

**Is credit card cloning really a problem?**

Yes. In fact, cloning has been the most popular form of credit card fraud over the past few years. It has grown 87% since 2010 and recently resulted in $6 billion in losses nationwide.

**Why is credit card cloning so popular?**

Credit card cloning is a popular identity theft tactic because it’s easy. Skimmers are easy to access and easy to use. Most are battery powered, allowing them to be used anywhere, and some are small enough to keep in your pocket. A gas station clerk can easily swipe your card through a pocket skimmer without you even realizing what happened.

**How do I protect myself?**

There are three major ways to protect yourself from credit card cloning. First, keep a close eye on where you’re using your debit or credit cards. Check the outsides of ATMs or gas station card readers before you place your card into the slot. If something looks strange, go to a new ATM, pump, etc. When you give your card to a cashier, make sure to keep an eye on your card at all times. Looking away for a second is enough time for them to swipe your card through a skimmer without you noticing.

Second, monitor your credit and debit card activity on a regular basis. Sign up for online access to your accounts and check them regularly for fraudulent purchases. Keeping a close eye on these items can help you determine if something is out of the ordinary.

Third, use cash. It seems silly, but it’s really the only way to keep you protected from credit card cloning.

Credit card cloning is a serious identity theft epidemic, and the more you know about it,  the more you’ll be able to keep yourself safe.

**Internet Security – Laws**