INFS 401
AUTOMATION OF INFORMATION SYSTEMS

INTERNET SECURITY: PROTECTION AGAINST VIRUSES

Lecturer: Prof. E.E Badu, Dept. of Information Studies
Contact Information: eebadu@ug.edu.gh

INTEGRI PROCEDAMUS

UNIVERSITY OF GHANA
College of Education
School of Continuing and Distance Education
2018

Session Outline

Topics to be treated in this session are;

- Viruses and Trojans
- Protection against viruses

By the end of this Unit, you should be able to

- Know what viruses and Trojans are
- Know the risk of exposure to malware
- Know how viruses spread
- Know who creates viruses
- Know how to avoid viruses

Topic One

VIRUSES AND TROJANS

VIRUSES AND TROJANS

What viruses and trojans are;

- A virus is a computer program that makes copies of its own program code, enabling it to spread like a disease.
- A Trojan is a similar type of threat to a virus, like a virus, a Trojan lodges unseen in the memory of your PC and does its nefarious business in secret.

VIRUSES AND TROJANS CONT’D

The difference between them is how the infection spreads. Virus infection typically comes from running an infected program, or booting your system is infected, the virus code then sets about subverting other programs or disks into vehicles for infection. Trojan work differently. Rather than attempting to covertly distribute their code, Trojans disguise themselves as legitimate programs. A classical Trojan relies on what is called social engineering to spread (It basically means exploiting human nature).

THE REASONS TO AVOID INFECTION

Reason why one has to avoid infection are as follows:

- **Poor Performance** – Many types of malware once they infect the computer eat up memory and CPU resources which would have been used for your own program. They degrade the PCs performance especially if the system has limited RAM and processing power.

- **Danger to Others** – Many types of malware are infectious so there is always the risk to pass them onto others and expose them to all hazards on the page.

THE REASONS TO AVOID INFECTION CONT’D

- **Disruption** – Malware can interface with the computer in unexpected ways for example, Trojan might deliberately hijack your web browser, in a bid to keep you away from certain sites and prevent you from installing software (typically malware around software.

- **Data Loss** – Malware creators deliberately wipe data from your machines, the virus can store a copy of your data in an encrypted form, which is then recovered if some form of payment is made for a decryption key. Since this is a dangerous business that could cause their arrests through the payments these days the creators have a purely destructive motive.

THE REASONS TO AVOID INFECTION CONT'D

- **Unexpected Phone Bills** – A certain class of viruses and Trojans called 'dialers' attack certain telephones especially late at night when people are asleep then they use your modem to call foreign premium numbers, running up enormous bills at one's expense.

- **Identity Theft** – Probably this is the biggest threat, a malicious program simply sits and watches as you visit all sorts of websites. The malware monitors the passwords you enter and keeps a record of the information that comes up on the screen. These details can then be transmitted to wherever the malware creator chooses.

THE REASONS TO AVOID INFECTION CONT'D

ESPIONAGE and Cyber-War – Malware attacks have been successfully used to steal secrets from corporations and governments. In 2011, a virus named StuXnet was even used to successfully sabotage Iran's nuclear programme. In May 2017 the National Health Services computers in the organization were not functioning as a result of virus attack.

SIGNS OF VIRUS INFECTION

The following are signs of virus and Trojan infections

- **Computer feels slow** – If a computer suddenly slows down for no apparent reason that could be a sign that a virus has made its home on the hard disk.

- **Some Files cannot be deleted** – A classic symptom of virus infection is there is a file on USB drive that you don’t recognize and try to delete it, only to find that you can’t. Either the virus is preventing you from removing it or its automatically re-infecting the disk as soon as it sees the original infection has been removed.

SIGNS OF VIRUS INFECTION CONT’D

- **PC crashes or freezes** – Viruses will not crash a PC on purpose, what they do is that they find it difficult to operate if windows and all other applications are up-to-date. They fail to work in the intended way and this causes the system to be unstable or freeze completely, a clue that something fishy is going on.

- **New icons on your desktop** – Sometimes some icons appear on your desktop which you have not created, for example, you might see “Click here for sexy pictures”. This is a sure sign that something has been meddling with your PC.

SIGNS OF VIRUS INFECTION CONT’D

- **Browser is hijacked** – Some viruses and Trojans can change your browser settings so that an unfamiliar home page appears when you open it. They may also try to add toolbars to your browser to spy on your activity.

- **UAC (User Account Control) and Firewall Warnings** – UAC prevents programs from accessing sensitive files without permission. Windows firewall does a similar thing, preventing unknown programs from accessing the network. So if you see an access request from either UAC or the Windows Firewall suggests something is trying to infect your PC or that something already has.

SIGNS OF VIRUS INFECTION CONT'D

- **Bounced Emails** – If one logs in to the email one day and finds it's full of 'bounce' reports – that is messages warning that an email he sent couldn't be delivered – that is cause for suspicion. This is caused by a rogue virus trying to mail out copies of itself.
- **Can't install windows updates or run antivirus software** - Malware writers hate windows update and they really hate antivirus software. So viruses and Trojans try to disable these services so they can go about their nasty business in peace. If one cannot run Windows Update, or cannot open his regular antivirus software that is a strong hint that something on his system does not want him to patch vulnerabilities or scan for malware.

Topic Two

PREVENTION OF VIRUSES

METHOD TO FOLLOW IF PC IS INFECTED

Most malware infections can be cleaned up without damaging your system. The following are a few tips if your PC is infected.

- **Change password** - Most malware attacks are intended to steal passwords and other personal information. So change the password to your primary email account.
- **Contact your bank** – If PC is used for online banking, there is the chance account details have been compromised. Call the bank and follow any procedures they tell you to restore order to your account.

METHOD TO FOLLOW IF PC IS INFECTED

- **Tell your friends** – Viruses spread, so if one has a virus, there is the likelihood that he will pass it on to a friend, or perhaps caught it from a friend who is not aware. As a courtesy he should warn anyone who has been exchanging files or links with him.
- **Perform an antivirus scan** – If an antivirus software is installed simply open the interface and start a complete scan of the system. Plug in any USB drives owned and see a full report of all malicious object found.

METHOD TO FOLLOW IF PC IS INFECTED

- **Start PC from a Boot CD** – If the last step does not solve the problem, perform a scan from a CD-based boot environment. Several free boot CDs are available for download, one popular one is AVG Rescue CD available from avg.com.
- **Run System Restore** – When a virus gets lodged so deeply in the PC and it cannot be removed by antivirus, Windows System feature may save the day. Open the START menu in Windows vista or Windows7 and type “SYSTEM RESTORE” a list of recent changes appears, click “SHOW MORE RESTORE POINTS” to see ones from more than a few days ago, choose one and click NEXT then the PC will be reverted to that State Personal documents will be intact.

APPLICATION OF E-PAPER CONT’D

- **Reinstall Windows** – If the virus is somehow managing to cling on even after running SYSTEM RESTORE then a fresh installation of Windows will be needed.

INFS 401
AUTOMATION OF INFORMATION SYSTEMS

INTERNET SECURITY: PROTECTION OF PRIVACY ON FACEBOOK

Lecturer: Prof. E.E Badu, Dept. of Information Studies
Contact Information: eebadu@ug.edu.gh

UNIVERSITY OF GHANA
College of Education
School of Continuing and Distance Education
2018

Session Outline

Topics to be treated in this session are;

- Protection of Privacy on Facebook
- Internet Security
- Protecting PC, Smartphones and Tablets

By the end of this section you should be able to

- Know the risks of using Facebook
- Know how to use Facebook as safely as possible

Topic One

FACEBOOK SECURITY

FACEBOOK SECURITY

Facebook is the largest social media site in the world, with more than 800 million active users. This makes it a great hub for connecting with old and new friends. Unfortunately, it also makes it an attractive target for criminals looking to harvest personal data. The risks involved in using Facebook are as follows:

FACEBOOK SECURITY CONT'D

IDENTITY THEFT

Facebook is a gold mine of personal information. When you browse through someone's profile there is a good chance that you will find his full name, date of birth, his hometown, schools he attended, wedding anniversary date etc. If he is connected to family members online his mother's maiden name can be worked out. This information may be open to abuse e.g. armed with all this information, a criminal may be able to phone a person's bank and persuade them that they were talking to the real account holder.

FACEBOOK SECURITY CONT'D

EXPOSING YOURSELF

Posting personal information and pictures exposes one to the general public. Just like personal information these updates may be more widely available than one can imagine and the consequences of sharing them can be serious. E.g. Tales of employers turning down job applicants because of incautious remarks they have made online. Some public sector workers have been fired or disciplined for posting material that is deemed to reflect poorly on their professionalism. On a positive note criminals have also been arrested as they revealed a lot of themselves on Facebook.

FACEBOOK SECURITY CONT'D

FRIENDS GIVING OTHER FRIENDS AWAY

Facebook's photo tagging picture means that by default, anyone can take a picture of another person perhaps in the compromising way, upload it to their own profile, and associate it with the one's account.

FACEBOOK SECURITY CONT’D

No Proof of Identity

After sourcing one’s settings so that only verified friends can access one’s details and see photos, a person may still be at risk. This is because on Facebook there is no way to be sure that all one’s friends are who they claim to be. People accept Facebook requests on the strength of very little information. Researchers have found that many Facebook users will accept friend requests from entirely fictitious individuals especially if they have attractive profile pictures or if they have to be old class mates. This fake accounts could easily be controlled by com men who all have access to all the same personal information as your true friends

FACEBOOK SECURITY CONT'D

Untrustworthy Apps

One of the key features that makes Facebook more than just a message board is its support for third-party apps. The ability to play games with friends adds a whole new dimension to social networking, but it can also be a liability. App developers typically make money by showing adverts within their apps, so it is in their interests to push as many people as possible to install and use them. To this end, many apps act almost like viruses: as soon as one of your friends installs and runs an app, it bombards all their friends with messages urging them to install the app themselves. This can be a real nuisance. Many apps also demand access to personal information before they will run. This information could end up anywhere.

FACEBOOK SECURITY CONT'D

Facebook changes constantly

Mark Zuckerberg has said that one of the core maxims of Facebook development is move fast and break things. True to his word Facebook is constantly evolving with new features appearing and old ones changing all the time. This keeps Facebook fresh and exciting. This comes with a price, it means security settings should also constantly change. New updates can compromise your security in unexpected ways. To stay safe, you must be alert and keep on top of new Facebook features as they appear.

Managing Facebook Security

Some of the most important ways of tightening privacy and security are as follows:

- **Limited Accounts** – This setting is under Account Settings - General. For privacy use this setting to unlink your accounts click the small downward arrow at the top right of Facebook. The result is that Facebook will not be linked to other services like Google and My Space.
- **Secure Browsing** – Located under Account Setting – Security. Turn this on to stop any one stealing your data.

Managing Facebook Security Cont’d

- **Login Notifications** – If security under Account Settings is turned on it also notifies you if someone tries to log into your Facebook account. It sends you an e-mail every time your account connects from a device you haven’t used before.
- **Control Default Privacy** – From the main PRIVACY SETTINGS set a default protection level for everything you post. Create a list of trusted friends’ accounts that is genuine by choosing the ‘CUSTOM’ privacy setting. So whatever you post will be visible to only the members in the list.

Managing Facebook Security Cont’d

- **Who can look you up** – Go to PRIVACY SETTING then ‘HOW YOU CONNECT’ to will restrict your personal information being accessed by anybody.
- **Public Search** – ‘Privacy Settings’ then choose APPS and WEBSITES then choose PUBLIC SEARCH, the last option, this will prevent people from finding your information.   Activity 4.1 Demonstrate the risk that Facebook poses to Internet Security

INFS 401
AUTOMATION OF INFORMATION SYSTEMS

DEVELOPING A COMPUTER-BASED INFORMATION SYSTEM PART 1

Lecturer: Prof. E.E Badu, Dept. of Information Studies
Contact Information: eebadu@ug.edu.gh

UNIVERSITY OF GHANA
College of Education
School of Continuing and Distance Education
2018

Session Overview

Developing a computer-based Information System is related to our study of INFS 308 Systems Analysis and Design, more or less an application of INFS 308. Developing Computer-based information system is about the methods that you will use to install computerized information systems in organization.

This part of the session however looks at other related issues. It covers five sections.

Session Outline

Topics to be treated in this session are;

- topic 1: Types of Automated Information Systems and Function Analysis
- topic 2: The Study of the Current System
- topic 3: Analysis of current systems

By the end of this Unit, you should be able to

- Choose the type of computerized information system you would like an organization to possess
- Study and Analyze an information system
- Propose an improved computerized information system for your organization
- Select hardware and software for an organization

Topic One

TYPES OF AUTOMATED INFORMATION SYSTEMS

INTRODUCTION

Upon completion of the section you should be able to:

- Know the options in automation
- Choose the type of automated system you deem fit for your organization
- Understand different types of automated systems, the origins and their capabilities

TYPES OF AUTOMATED INFORMATION SYSTEMS

There are different options these days when it comes to Automating information systems. Some include internet-based services, outsourcing, customer solution from Information Technology consultants and enterprise-wide software strategies as well as open some systems. However all these fall under two broad categories namely,

- Systems sold by firms to organizations
- Systems developed in-house or co-operatively on cost-sharing not-for-profit basis.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT'D

- **In-House Developed Systems** – This is an information system designed for a particular organization by someone contracted to do so or designed by a member of staff for the organization. It is the organization that owns the system and therefore has the copyright. Methods adopted conform to system analysis and design principles of understanding a system problem, analyzing and designing a new system.
- For large information systems, some organizations may decide to co-operate to develop and share the system. Co-operation is achieved at three levels:
- Sharing the cost of the system development
- Sharing database
- Sharing hardware. An example of the co-operatively shared system is CDS/Isis which was developed by UNESCO.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT'D

SYSTEMS SOLD BY FIRMS

These can be systems outsourced, systems developed by IT organizations such as iii, innovative etc., and sold to organizations such as University of Ghana or University of Michigan.

- Others are also off-the shelf packages and are mostly turnkey systems. A turnkey system means a system supplied completely with hardware and software to the purchaser's specification and installed ready for operation. In other words, by turning the key, the system becomes operational.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT’D

Cooperate turnkey standalone systems also exist where an organization develops a system that gives local control to the shared members but the product is the same for all the participating organizations who pay a yearly subscription fee. Example is Sierra and Millenium developed by Innovative Group.

In some cases, some systems are customized for the organization (bespoked). Other organizations also sell software only. Some software only systems are text retrieval and database products such as Status, Basis and Revelation.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT’D

FUNCTION ANALYSIS

- Some or most large information systems are made up of many subsystems. In some cases especially in developing countries some organizations cannot afford to automate all the functions in one go so some sort of priority selection will have to be made by doing a needs assessment. The needs of the organization are analyzed and measured against current functions. By this method some functions will be found obsolete and the important ones that agree with the current vision of the organization are prioritized using FUNCTION ANALYSIS.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT’D

Function Analysis is a method used for selecting the function among many that require priority automation. It does so by actually recording information system functions by using a specially designed table to select priority functions needing automation.

On the scale of 1 – 10 where 1 is the minimum and 10 the maximum columns in the table are completed. See Table 3.1

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT’D

Table 3.1 FUNCTION ANALYSIS

Information System Function	Priority	Backlog or Bottle-neck	Repetitive Action	Labour Intensive	Accuracy Vital	Location Problem	Time Vital	Total
Life Insurance	7	6	3	5	6	5	8	40
Fire Insurance	8	7	4	3	6	5	8	41
Motor Insurance	6	6	2	3	6	4	8	35

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT'D

- In column 1 functions in relation to goals and objective of the information system are listed. Column 2: Under priority, assess the priority by looking at how essential to the goals and objectives of the information system a particular function is. Here consensus among staff is necessary as priorities may differ from staff to staff.
- Column 3: Backlog and Bottlenecks – these refer to constraints with a particular function that are affecting other functions.
- Column 4: Repetitive function – Many information system functions are highly repetitive so the function that is highly repetitive is a more suitable candidate for automation.
- Column 5: Labour Intensive – there is a decision on the function that is labour intensive.
- Column 6: Accuracy Vital – many information system work demand high accuracy, for example, recording of financial data invoices.

TYPES OF AUTOMATED INFORMATION SYSTEMS CONT'D

- Column 7: Location Problems- you have to identify problems with material location.
- Column 8: Time Vital – immediate response to many enquiries. Functions that require rapid response.
- Column 9: This is the total column. The higher that number the more likely that function is a candidate for automation.
- Using Table 3.1 the columns are filled as illustrated. The function with the highest number in column 9 becomes the first function to be automated followed by the next highest number and so on.
- From the table fire insurance system has the highest figure so it becomes the first function to be automated in an Insurance Information System.
- After the selection of functions to be automated, the next step is to find appropriate computer-related technologies that can be used to perform these functions.