**UNIVERSITE POLYTECHNIQUE DE BINGERVILLE**



***LICENCE 3 in CYBER SCIENCES***

***Dr secredou***

**ENGLISH COURSES FOR INTERMEDIATES**

**FORWARD**

Our general English courses tailored for intermediates will provide students with strong background in every aspect of the language. Each lesson has clear objectives that constitute the overall progress of the learners. It introduces basic grammar, essential vocabulary, and help to acquire practical communicative skills on daily topics.

There are opportunities for individual, pair and group work and private study at home. This book includes a wide range of activities and approaches designed to appeal to different personal learning styles.

The course consists of 5 units, each containing the same component sections which cover various types of activities.

**UNIT 1**

**CV AND APPLICATION LETTER**

1. **INTRODUCTION**

CV stands for curriculum vitae, which means a brief account of your career. CVs are used to explain to recruiters what you can do and what you have done, so a good CV looks forwards as well as accounts for what you did in the past.

1. **CONTENT OF CV**

A CV needs to include enough information for the recruiter to decide whether you are likely to be a suitable candidate. It may include the following:

* **Personal details** - name, age, address, mobile phone number, email address.
* **Educational**: academic or professional qualifications, dates of institutions attended.
* **Professional experience** – date of previous jobs title, tasks and employers (previous companies);
* **Skills and competencies** – IT, language and additional (driving licence).
* **Hobbies**: reading, swimming, dancing, etc. It also includes membership of an association.
* **References** – at least three people (name, title and company or institution).

1. **APPLICATION LETTER**

A letter of application typically provides detailed information on why are you qualified for the job you are applying for.

**CONTENT OF AN APPLICATION LETTER**

A possible format for your letter is as follows:

* **YOUR NAME AND ADDRESS** : In CAPITAL letters
* **THE DATE** : Use long date, e.g. 30 October 2010
* **SALUTATION**

Dear Mr/ Mrs/ Ms/ Miss Jones

Dear Jack

Dear Sir

Dear Madam

Hi Jerry

My darling Linda

* **REASONS FOR WRITING**

In response to a job advertisement Internship

* **WHO YOU ARE**

Distil five lines from your resume.

Include your latest qualification or the details of the degree you are currently completing

Mention the University and any majors studied and a project or interest area if relevant

* **MARKETING YOURSELF**

Experience/skills developed which are relevant;

Include reasons for wanting this particular job;

Any benefits you bring to the job or company;

* **ANY ADDITIONAL DOCUMENT**

Resume, selection criteria, academic record

Provide details on how to contact you

How, when, and where you can be contacted for an interview

* **CLOSURE**

Yours sincerely

Yours

Yours faithfully

(With) Best wishes

See you soon

Hear from you soon

Kind regards

**ASSIGNMENT**

**MATCHING QUESTIONS 1**

Fiona Scott is one of the applicants for the job at Patagonia. Study her CV carefully to see how the information is presented and decide where each of the following headings should be placed.

**REFERENCES INTERESTS PERSONAL DETAILS**

**PROFESSIONAL EXPERIENCE EDUCATION ADDITIONAL SKILLS**

CURRICULUM VITAE

…………………………………………

**PHOTOGRAPH**

Name Fiona Scott

Date of Birth: 7 August 1969

Nationality: British

Address: 52 Hanover Street

Edinburgh EH2 5LM

Scotland

Telephone: 031 449 0237

Email: fionascott@xxx.com

………………………………………………..

1991-1992: London Chamber of Commerce and Industry Diploma in Public Relations

1988-1991: University of London

BA (Honours) In Journalism and Media Studies (Class П)

1981-1988: Fettes College, Edinburgh

A-levels in German (A), English (B), History (B) and Geography (C

………………………………………

1995 to present: Scottish Wildlife Trust Department of Public Relations

Responsible for writing articles on all aspects of the Trust's activities and ensuring their distribution to the press. Editor of the Trust's monthly journal. In charge of relations with European environmental agencies.

1992-1995 Press Officer, Highlands Tourist Board Preparation of promotional materials

and brochures Co-ordination of media coverage

Summer of the Glasgow Tribune newspaper 1990 and 1991 Two three –month training periods as assistant to the Sports Editor Arranging and conducting interviews Preparation of articles covering local community sports events

……………………………….

IT Office 2000 and Windows NT, Excel, Internet, PowerPoint Languages Fluent German and proficient in French Additional Driving licence ( car and motorcycle)

…………………………………

Cross-country skiing, rock-climbing and swimming Ski instructor (grade II) Secretary of the local branch of ‘Action’, an association organizing sports activities for disabled children

………………………………………

Geoffrey Williams Brenda Denholm Professor of Journalism Sports Editor University of London The Glasgow Tribune

**UNIT 2**

**Employment Rights & Data Protection**

1. **INTRODUCTION**

Employment law covers all rights and obligations within the employer-employee relationship -- whether current employees, job applicants, or former employees. Because of the complexity of employment relationships and the wide variety of situations that can arise, employment law involves legal issues as diverse as discrimination, wrongful termination, wages and taxation, and workplace safety. Data Protection Act (DPA) is a law designed to protect personal data stored on computers or in an organized paper filing system which is also very important in managing people today.

1. **EMPLOYEE RIGHTS IN THE WORKPLACE**

All employees have basic rights in the workplace -- **including the right to privacy, fair compensation, and freedom from discrimination**. A job applicant also has certain rights even prior to being hired as an employee. Those rights include the right to be **free from discrimination based on age, gender, race, national origin, or religion during the hiring process**. For example, a prospective employer cannot ask a job applicant certain family-related questions during the hiring process.

In most states, employees have a right to privacy in the workplace. This **right to privacy applies to the employee's personal possessions, including handbags or briefcases, storage lockers accessible only by the employee, and private mail addressed only to employee.** Employees may also have a right to privacy in their **telephone conversations** or **voicemail messages**. However, employees have very limited rights to privacy in their e-mail messages and Internet usage while using the employer's computer system.

There are certain pieces of information that an employer may not seek out concerning a potential job applicant or employee. An employer may not conduct a credit or background check of an employee or prospective employee unless the employer notifies the individual in writing and receives permission to do so.

**Other important employee rights include:**

* Right to be free from discrimination and harassment of all types;
* Right to a safe workplace free of dangerous conditions, toxic substances, and other potential safety hazards;
* Right to be free from retaliation for filing a claim or complaint against an employer (these are sometimes called "**whistleblower**" rights);
* Right to fair wages for work performed.

1. **THE NEED FOR THE DATA PROTECTION ACT**

During the second half of the 20th century, businesses, organisations and the government began using computers to store information about their customers, clients and staff in databases. For example:

* names
* addresses
* contact information
* employment history
* medical conditions
* convictions
* credit history

Databases are easily accessed, searched and edited. It’s also far easier to cross reference information stored in two or more databases than if the records were paper-based. The computers on which databases resided were often networked. This allowed for organisation-wide access to databases and offered an easy way to share information with other organisations.

The [**Data, information and databases**](http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/) section has more on [**searching databases**](http://www.bbc.co.uk/schools/gcsebitesize/ict/databases/2databasesrev5.shtml).

**Misuse and unauthorised access to information**

With more and more organisations using computers to store and process personal information there was a danger the information could be misused or get into the wrong hands. A number of concerns arose:

* Who could access this information?
* How accurate was the information?
* Could it be easily copied?
* Was it possible to store information about a person without the individual’s knowledge or permission?
* Was a record kept of any changes made to information?
* **Types of personal data**

Some data and information stored on a computer is personal and needs to be kept confidential.

Two types of personal data

Personal data is about living people and could be:

• their name

• address

• medical details or banking details

Sensitive personal data is also about living people, but it includes one or more details of a data subject's:

• racial or ethnic origin

• political opinions

• religion

• membership of a trade union

• health

• sex life

• criminal activity

There are fewer safeguards for personal data than there are for sensitive personal data. In most cases a person must be asked specifically if sensitive data can be kept about them.

* **The rights of data subjects**

People whose personal data is stored are called data subjects. The DPA sets up rights for people who have data kept about them. You need to know these rights for the exam. They are:

**A Right of Subject Access**

A data subject has a right to be supplied by a data controller with the personal data held about him or her. The data controller can charge for this (usually around £10 pounds).

**A Right of Correction**

A data subject may force a data controller to correct any mistakes in the data held about them.

**A Right to Prevent Distress**

A data subject may prevent the use of information if it would be likely to cause them distress.

**A Right to Prevent Direct Marketing**

A data subject may stop their data being used in attempts to sell them things (eg by junk mail or cold calling.)

**A Right to Prevent Automatic Decisions**

A data subject may specify that they do not want a data user to make "automated" decisions about them where, through points scoring, a computer decides on, for example, a loan application.

**A Right of Complaint to the Information Commissioner**

A data subject can ask for the use of their personal data to be reviewed by the Information Commissioner who can enforce a ruling using the DPA. The Commissioner may inspect a controller's computers to help in the investigation.

**A Right to Compensation**

The data subject is entitled to use the law to get compensation for damage caused ("damages") if personal data about them is inaccurate, lost, or disclosed.

1. **THE IMPORTANCE OF DATA PROTECTION IN TODAY’S BUSINESS WORLD**

In today’s highly technological world, data protection is more important than ever. It is vital that companies do everything that they can to protect the information that is maintained in their computer systems. Hackers are everywhere, and while some system break-ins are purely for kicks and bragging rights, others are done with the intent of utilizing stolen data for personal gain.

Businesses have an obligation to safeguard any data supplied to them by consumers, including basic identity information (such as names, addresses, phone numbers and birth dates), as well as more sensitive data (such as social security numbers, medical records, and credit card numbers).

The duty to protect data goes beyond even the personal information, as stated above. For certain companies, it includes patents, concepts and ideas that could be worth hundreds of thousands of dollars, if not more. Ultimately, the list of information that requires protection can be quite large.

The consequences of not using proper data protection can be extremely harmful to individuals and businesses alike. A popular use of such stolen information is identity theft and when it occurs, people often end up inconvenienced or worse, often battling with credit agencies and companies over the misuse of their names, social security numbers, and credit card information. Expunging records is time-consuming and can get in the way of customers paying their bills, buying groceries, and handling other financial necessities

**ASSIGNMENT 1**

* 1. **Write SHORT notes on the following:**
     1. Employment right
     2. Employment law
     3. Data Protection Act
     4. Whistleblower
     5. Data
     6. Information
  2. Which types of information do companies, organizations and governments seek to protect the most?
  3. Why data protection data is so important for our world today?

* 1. What are the consequences of poor data protection?

**ASSIGNMENT 2 (Multiple choice format)**

**1. A worker is dismissed because of his religion: what is this an example of ?**

**a. Redundancy**

**b. Unfair dismissal**

**c. Health and safety at work**

**2. A worker is dismissed because the business the business is changing its organizational structure: what is this an example of ?**

**3. Staff are sent home because of local flooding: what is this an example of ?**

**a. Redundancy**

**b. Unfair dismissal**

**c. Health and safety at work**

**4. What is redundancy?**

**a. When a business dismisses workers unfairly**

**b. When a worker dismisses workers fairly**

**c. When a business sends workers home on unpaid leave.**

**5. Why can redundancy occur?**

**a. Because a business introduces new technology**

**b. because a business needs to cut costs**

**c. both of the above answers**

**MATCHING QUESTIONS 2**

**COMPLETE FIONA SCOTT’S LETTER OF APPLICATION USING THE FOLLOWING VERBS:**

**Contact – discuss – apply – enjoy – employed – notice – welcome – advertised – involved – matches.**

Fiona Scott

52 Hanover Street

Edinburgh EH2 5LM

Scotland

UK

5th January

Nathalie Baudoin

Patagonia GMBH

8000 Munich 22

Germany

Dear Ms Baudoin,

I am writing to **1** -------APPLY-- for the position of Public Affairs Associate which was 2 ---ADVERTISED------last week in the International Herald Tribune.

Although I am presently **3** --------- by a non-profit making organization, it has always been my intention to work in a commercial environment. I would particularly **4** --------- the chance to work for your company and as you will **5** ----------- on my enclosed curriculum vitae, the job you are offering **6** ------------ both my personal and professional interests.

My work experience has familiarized me with many of the challenges **7**------------ in public relations today. I am sure that this, together with my understanding of the needs and expectations of sport and nature enthusiasts, would be extremely relevant to the position.

Moreover, as my mother is German, I am fluent in this language and would definitely **8** ------------ working in a German-speaking environment.

I would be pleased to **9 -**-------- my curriculum vitae with you in more detail at an interview. In the meantime, please do not hesitate to **10** ----------- - me if you require further information. I look forward to hearing from you.

Yours sincerely,

Fiona Scott

**UNIT3: SMARTPHONE SECURITY**

INTRODUCTION

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wifi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator. So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer. Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks. For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone).However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed. It's worth reviewing all the risks associated with mobile phones discussed in our guide How to use mobile phones as securely as possible as all of them are also relevant to smartphone use. That guide also covers issues of eavesdropping, interception of SMS or phone calls, SIM card related issues, and best practices. In this guide we'll take a look at the additional security challenges posed by smartphones.

SMARTPHONE SECURITY GUIDELINES

Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

A simple exercise can help illustrate this:Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find: - Pictures of loved ones (~5 pictures) - Identification cards (driver's license, membership cards, social security cards) - Insurance and health information (~2 cards) -

Money (~5 bills) - Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

Pictures of loved ones (~100 pictures)

Email applications and their passwords

Emails (~500 emails)

Videos (~50 videos)

Social networking applications and their passwords

Banking applications (with access to the bank accounts)

Sensitive documents

Sensitive communication records

A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold. It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency. In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

Platforms, Setup and Installation

Platforms and Operating Systems

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (FOSS) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter. Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as GPS or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too. Blackberry phones have been presented as “secure” messaging and email devices. This is because messages and emails are securely channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

Feature Phones

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for security applications or improvements. We do not specifically address feature phones,although many measures discussed here make sense for feature phones too.

Branded and locked smartphones

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone. For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

General Setup

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

Installing and updating applications

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices. The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you should look for alternative applications with appropriate access and rights.). Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is F-Droid ('Free Droid'), which only provides FOSS applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store. If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending .apk files (short for 'android application package') via bluetooth. Alternetively you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (Note: be especially careful while using Bluetooth.

Communicating Securely(Through Voice and Messages) with a

Smartphone

Secure Voice Communication

Basic telephony

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence25. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time. About Anonymity: If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

 Make calls from different locations each time, and choose locations that are not associated with you.

 Keep your phone turned off, with the battery disconnected, go to the chosen location,switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.

 Change phones and SIM cards often. Rotate them between friends or the second-hand market.

 Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you. About eavesdropping: Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

 Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.

 If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.

 Make sure that any person with whom you communicate also employs the safeguards

described here.

 In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen. About interception of calls: Typically, encryption of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications. It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones. Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place26. Using Internet through your Smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using VoIP and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well (See Redphone below). Here we list a few tools and their pros and cons:

Skype

The most popular commercial VoIP application, Skype, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections. Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

Other VoIP tools

Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate. RedPhone is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use, RedPhone uses your mobile number as a way to identify you to your contacts. Unfortunately, this makes it more difficult to use RedPhone without a functioning mobile service plan, even on devices capable of using WiFi to connect to the Internet. RedPhone also uses a central server, which puts the administrators of the service in a powerful position by allowing them to see much of the meta-data related to your encrypted VoIP calls. CSipSimple is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different VoIP services. Open Secure Telephony Network (OSTN) and the server provided by the Guardian project, ostel.co, currently offers one of the most secure means to communicate via voice. Knowing and trusting the entity that operates the server for your VoIP communication needs is an important consideration. When using CSipSimple, you never directly communicate with your contact, instead all your data is routed through the Ostel server. This makes it much harder to trace your data and find out who you are talking to. Additionally, Ostel doesn't retain any of this data, except the account data that you need to log in. All your speech is securely encrypted and even your meta data, which is usually very hard to disguise, is blurred since traffic is proxied through the ostel.co server. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use. Tool Guides for CSipSimple and Ostel.co are forthcoming. In the meantime, more information can be found by following the links above.

Sending Messages Securely

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

SMS

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

Securing SMS

Text Secure is a FOSS tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. Text Secure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to tamper with the contents of a message. In our Text Secure hands-on guide we explain in detail the features of this tool and how to use it.

Secure Chat

Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting. There are ways to chat and instant message securely. The best way is to use end-to-end encryption, as this will enable you to make sure the person on the other end is who you want. We recommend ChatSecure as a secure text chat application for the Android phones. ChatSecure offers easy and strong encryption for your chats with Off-the-Record Messaging protocol. This encryption provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure. ChatSecure has been designed to work together with Orbot, so your chat messages can be routed through the Tor anonymizing network. This makes it very hard to trace it or even find out that it happened. For iPhones, the ChatSecure client provides the same features, although it is not easy to use it with the Tor network. Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

Storing Information on your Smartphone

Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. You can take steps to encrypt any sensitive information on your phone by using specific tools.

Date Encryption Tools

The Android Privacy Guard (APG) allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

Recording Password Securely

You can keep all your needed passwords in one secure, encrypted file by using Keepass. You will only need to remember one master password to access all the others. With Keepass you can use very strong passwords for each account you have, as Keepass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise Keepass password databases between your phone and your computer. We recommned that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and syncronise this one instead of coping an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very strong password for your Keepass database.

Sending Email from your Smartphone

In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion. If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

 Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.

 If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands. Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encrytpion key-pair (using APG) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

Capturing Media with your Smartphone

Capturing pictures, video or audio with your Smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful: Have a mechanism to securely upload recorded media files to protected online location and remove them from the phone instantly (or as soon as you can) after recording. Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device. Protect or remove meta information about time and place within the media files. Guardian Project has created a FOSS app called Obscura Cam to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscura cam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

Accessing the Internet Securely from your Smartphone

As discussed in our guide How to keep your Internet communication private and our guide How to remain anonymous and bypass censorship on the Internet, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

Through Wi-Fi or Mobile Data

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator. Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers. In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers. Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

Anonymity of your Smartphone

To access content online anonymously, you can use an Android app called Orbot. Orbot channels your internet communication through Tor's anonymity network. Another app, Orweb, is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

Proxies

The mobile version of Firefox – Firefox mobile can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. We recommend the Proxy Mobile addon (also from Guardian Project, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the Tor network.

**UNIT4 : EMAIL AND SOCIAL MEDIA SECURITY**

Introduction

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site. Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you? Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it. If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with. Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

General Tips on using Social Networking platforms safely

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media. Always ask the questions: ⎫ Who can access the information I am putting online? Who controls and owns the information I put into a social networking site? What information about me are my contacts passing on to other people? Will my contacts mind if I share information about them with other people? Do I trust everyone with whom I'm connected? Always make sure you use secure passwords to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine. Make sure you understand the default privacy settings offered by the social networking site, and how to change them. Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible. Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine. ¬ Access social networking sites using https:// to safeguard your username, password and other information you post. Using another layer of security by encrypting the traffic from your browser to your social networking site. Be careful about putting too much information into your status updates – even if you trust the people in your networks. It is easy for someone to copy your information. Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly careful when integrating your social network accounts! You may be anonymous on one site, but exposed when using another. Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

Posting Personal Details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands. Ask yourself: is it necessary to post the following information online? ⎫ birth dates ⎫ contact phone numbers ⎫ addresses ⎫ details of family members ⎫ sexual orientation ⎫ education and employment history

Friends, Followers and Contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have. 126 When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

Status Updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else. To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you. There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

Sharing Online Content

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution. If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

Revealing your Location

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings. Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

Sharing Videos and Photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first. Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

Instant Chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about. Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure). It is more secure to use a specific application for your chats, such as Pidgin with an Off-therecord plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

Joining and Creating Groups, Events and Communities

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk? When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you? Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

EMAIL SECURITY TIPS

Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program. 2. You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is Tor (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.

You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.

You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.

Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.

Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

ACTIVITY 1.

What are anonymous accounts? Find some browsers which supports anonymouity. 2. After going though the above section, find out whether you were following the above safe pracitices while handling your social medial account? Find the gaps? 3. Based on the above recommendations, adjust your social media account settings.

**UNIT 5**

**WRONGDOING AND CORRUPTION**

**PARADISO FINANCIAL SERVICES**

**REGULATORY AUTHORITY**

We regulate financial services;

 Our job is to prevent financial wrongdoing and punish the wrongdoers.

* **Insider dealing or insider trading**:   
  someone buys or sells securities using information that is not publicly available.

Chinese walls are measures that you can take to stop knowledge in one department of your company being illegally used by another department, to buy or sell shares for example.

* **Price fixing:** a group of companies in the same market secretly agree  to fixe prices at a certain level, so they do not have to compete with each other.
* **Market rigging:** a group of investors work together to stop a financial market functioning as it should, to gain an advantage for themselves.

**BRIBERY AND CORRUPTION**

An illegal payment to persuade someone to do something is a bribe, or informally a backhander **(BrE only),** kickback or sweetener.

 To bribe someone is bribery.

 Someone who receives bribes is corrupt and involved in corruption.

 This is informally known as sleaze, especially in politics.

**FRAUD AND EMBEZZLEMENT**

I’m Sam Woo.

 I've been a fraud squad detective for 20 years and I've seen a lot !

Once, a gang counterfeited millions of banknotes in a garage.

 We found US$10million in counterfeit notes.

 They were very good quality.

 Counterfeiting or forgery of banknotes was a problem, but now all the forgers are in jail.

Faking luxury goods like Rolex watches was also a problem, but we're w-orking hard to close workshops where fakes are made.

There have been bad cases of fraud where someone offers to lend mone-y, but demands that the borrower pays a "fee" before they get the loan.

 People can be stupid.

And there's embezzlement, a type of fraud where someone illegally gets money from their employer.

 One accountant sent false invoices to the company heworked for, and paid money from his company into bank accounts of false companies he had "created".

 He embezzled $2 million - quite a scam.

There used to be a lot of racketeers demanding "protection money" frombusinesses.

 If they didn't pay, their businesses were burnt down.

Money laundering, hiding the illegal origin of money, is common - gangsters buy property with money from drugs.

 When they sell the property, the money becomes "legal".

 But banks now help by telling us when someone makes a large cash deposit.'

**ASSIGNMENT**

 ANSWER THE QUESTIONS USING EXPRESSIONS

1. Two ferry companies with ferries on the same route secretly meet in or-der to decide the prices they will charge next summer.

 What are they guilty of?

2. A company that wants to keep its share price high makes secret payments toinvestors who buy its shares.

 What are the company and the investors guilty of?

3. A rich businessman lends $1 million to a politician so that he can buy a house.

The politician pays no interest on the loan and does not mention it when asked to give a complete account of his finances.

 Which word, used especially about politicians, do people use to talk about this?   
4. Specialists in one department of a financial institution are advising Company X on a merger with another company.

 In another department of the financial institution, traders hear about this and buy large numbers of Company X's shares.

 What are they guilty of ?

 (2 expressions) What should the financial institution do to prevent this?  
5. A company selling weapons to a foreign government makes secret  payments to politicians who make decisions on which companies to buy  arms. **What could these payments be called? (4 expressions)**

**What is the company and the government guilty of? (2 expressions)**

**6. Complete this table, using information from C opposite. The first row has been done for you. You may wish to refer to a dictionary.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Noun:**  **crime** | **Noun:**  **criminal** | **Verb: what the criminal does(He/She)** | **Noun: thing**  **Made or done in the crime** | **Related adjective** |
| ***Embezzlement*** | ***embezzler*** | ***embezzles*** | ***embezzlement*** | ***embezzled*** |
| **Faking** | **faker** | **fakes** | **A fake** | **faked** |
| **Forgery** | **forger** | **forges** | **A forgery** | **forged** |
| **Fraud** | **fraudster** | **defrauds** | **A fraud** | **fraudulent** |
| **Money laundering** | **Money launderer** | **Launders money** | **-** | **-** |
| **Racketeering** | **racketeer** | **racketeers** | **-** | **-** |