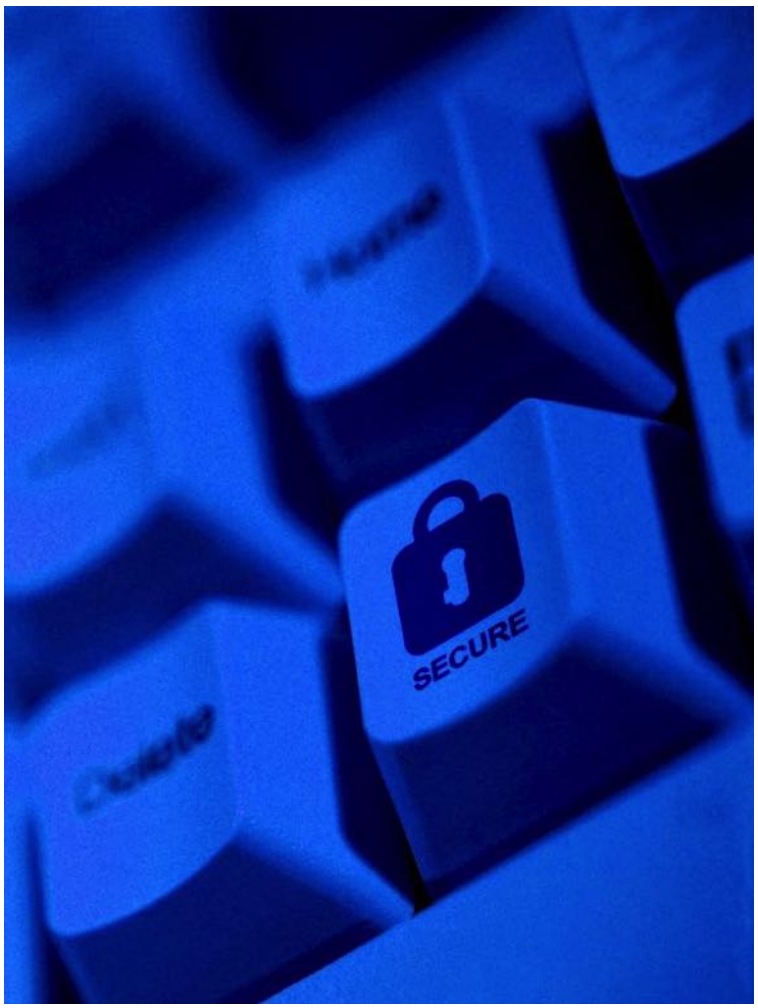
CAPITA
LEARNING & DEVELOPMENT

Group Risk

Security Awareness Training 2010 – 2011



Information Security Awareness

CAPITA
LEARNING & DEVELOPMENT

Table of contents

1. Background ……3
2. Introduction 4
3. John's story 5
4. Alice's story ……7
5. Stranger in the pub 9
6. Graham's story ……12
7. Jane's story 20
8. Sarah's story 23
9. Anonymous caller 27
10. In the coffee shop 29
11. Summary 30

CAPITA
LEARNING & DEVELOPMENT

1. Background

Meet Emma.

“At first, I didn’t really grasp the extent of it … When my credit card company called me to ask me whether it was me who had booked airline tickets over the phone for four flights, it was clear that somehow my credit card had been used without my knowledge. But how? It had never been out of my sight. As the weeks went by, it turned out that someone had my passport, my driving license … had taken over my bank and savings accounts … and had crashed in my insurance policy. Every day, some other piece of my life seemed to fall apart as I learned of another fraud committed in my name. My whole identity had been hijacked. Of course, I had read about situations such as these, but I had dismissed what I had read. You never really think it could happen to you. But it did happen to me. In fact, it happened to hundreds of others too. And it could just as easily happen to YOU!”

CAPITA
LEARNING & DEVELOPMENT

2. Introduction

During this module, you will learn that as Emma went about her day to day business, she:

- Purchased an insurance policy, paying the premium by credit card
- Advised her employer that she was changing her bank account and that future salary payments should be paid into her new account.
- Talked with her local council about her recent council tax payments.

As you work through this module, you will follow her as she engaged in each of these activities and will meet a number of the people with whom she talked. As you discover how they worked and what they did, light will be shed on how she fell victim to financial crime and identity theft.

Emma recalls taking out insurance by phone – find out what happened.

3. John's story

John's account of what happened is shown in an extract from his written statement which is now held on file.

"I was just doing my job! I took a call from a customer, Emma Mullen. She was enquiring about an insurance policy. I took some information from Emma so that I could enter it to the system, calculate the premium and answer her query. Emma accepted the quote and asked if the insurance would be effective immediately. I told her that was fine as long as she paid the premium by credit or debit card. Emma opted to pay by credit card but just as I was about to take her credit card details, my screen froze. Whatever I tried, I was unable to unfreeze my screen. It's not the first time this has happened whilst I've been in the middle of a customer call. I just did what we all do when the screen freezes. I noted down all her details on a jotter so that I could enter them on to the system as soon as it became available again. Nothing wrong with that, surely?"

Now look at the information John noted on the jotter. Decide whether or not what he has noted down puts Emma at risk of someone stealing her details and defrauding her.

Full name
Not a risk on its own

Full address
Not a risk on its own

Phone number
There is a risk that criminals could target Emma by phone pretending to be from legitimate companies or organisations and try to extract further personal information from her that they can subsequently use to steal her identity or her possessions

16 digit card number
Whilst it is unlikely that anyone could make a purchase against Emma's credit card with just her long card number, fraudsters are past masters at piecing together seemingly unconnected items of information. If they have Emma's name, address, telephone number and 16 digit card number, they have every incentive to find out the rest of what they need to make purchases in her name. It is not unheard of for criminals to call their targets themselves, claiming to be phoning from the victim's bank, and extracting passwords and other security information which they then use.

Issue date / expiry date
This is now becoming very high risk

3 digit security card number from the signature strip of the card
A fraudster now has everything they need to make purchases online or by telephone. Emma is at serious risk if this sheet of information falls into unscrupulous hands

Amount to be deducted
This could be of use to a fraudster if it was a significant sum since it would give the criminal a clue as to how much they could spend on Emma's card without exceeding her credit limit and so raising the suspicions of the credit card company.

You read through more of John's statement in which he says:

“Once the screen became available to me again some minutes later, I entered Emma’s credit card details that I’d noted on my jotter on to the screen and not wanting to leave these lying around, I tore the sheet from the jotter and threw it into the bin under my desk.”

John was not alone in the office. Other people are there. Where might the risks lie?

John’s colleagues
We generally trust our colleagues implicitly and we probably have no grounds to be suspicious of any of them. However, Emma and other customers put their trust in us when they give us their credit card details and other personal information and we have an obligation to honour that trust. Never place temptation in anyone’s way

Customers visiting the building
We tend, when we leave papers on our desks, to forget that our colleagues may not be the only ones to have access to the office. Customers and other individuals can also visit offices and be shown around. Credit card details left lying around may be too tempting for a visitor to resist copying down; leaving them lying around puts Emma at risk

Cleaners
There are many workers who visit offices whether they are cleaners, maintenance engineers, contractors watering the office plants, etc. Never leave temptation in their way.

John himself
John is a quiet type. He always keeps himself to himself. Occasionally he goes out with the team after work to the local pub but he never seems to buy a round of drinks. Then just last week, he suddenly seemed to have a wallet full of cash. Did he win the lottery or has he taken advantage of the credit card details that pass through his hands?

So Emma’s credit card details are now in the bin under John’s desk. You might think that once the paper they are written on goes into a refuse vehicle, it will not be possible to retrieve it. But there is no protection for Emma if on a windy day, her credit card details fall out the back of the refuse vehicle and blow down the street. Whenever personal information is copied, however it is copied, we risk it falling into unscrupulous hands.

Personal and commercial information should always be placed in the confidential waste bins to ensure secure disposal by the Group’s secure disposal provider. At home, ensure you shred any documents that contain your personal information by using a cross-cut shredder.

4. Alice's story

Meet Alice. She is meticulous about securing her workstation. She never leaves files or folders visible when she is away from her desk; she locks them away. Her Blackberry is always in her hand or in her bag, which she carries with her when she moves away from her desk. Yet a number of people seem recently to have accessed her system – the only way they could have done so, is if they had known her password. Alice is adamant that she has not divulged it to anyone, and she has recently changed it. Since around 50% of people use names of family members, names of pets or memorable dates such as birthdays, it might not have been too difficult for someone to have guessed Alice's password.

Even when a PC is left unsecured, clues to passwords are often left lying around on otherwise organised desks. Recent research shows that anywhere up to 50% of people use family names, dates of birth, names of pets, months of the year, etc as passwords. This means that anyone with criminal intent can fairly easily access systems, bank accounts, personal information and commit financial crime, with very little real effort. Research published in 2009 indicates that in the UK alone, 18 million people, (that is nearly 40% of all adults in the UK), are at risk of fraud because they use the same passwords for online banking, shopping, social networking and then re-use those passwords at work, putting at risk their customers and their colleagues too. So, if you have put your date of birth and the names of your pets on any of the social networking sites and you use them as passwords, you might want to quickly change your passwords, or better still, change your passwords and remove that information from the social networking sites!

Remember:

- Always keep passwords secret
- Don't write passwords down for others to find
- Don't leave clues to passwords lying around
- Choose 'complex' passwords that are difficult for others to guess. These typically combine capital and small letters, as well as numbers.
- Protect yourself! Protect your family! Protect your colleagues! Protect your customers! Protect the business! You wouldn't leave your front door open in the morning when you leave your house! Don't allow people access to your computer!

As you investigate how Emma may have fallen victim to financial crime, you learn that Alice does everything she possibly can online, both at work and in her private life. She is well and truly an example of what it means to live in the digital age. She's quite an organised person and avoids leaving paperwork lying around whether at work or at home – she likes things tidy. That means that when she's at work, everything gets recorded on her laptop. Meetings are written up on her laptop. Contacts and appointments are logged in Outlook. At home, she shops online, she banks online, she files her tax returns online. She provides annual updates to the local council for the electoral register online. She is registered with social networking sites and is linked to hundreds of friends around the world. She feels quite safe online. She knows her company has very sophisticated IT systems which maintain a high degree of security. And at home, she has antivirus software installed. But you learn that when Alice was interviewed as part of the investigation into fraud, she reported that she had recently received a private email from a friend who worked in another company:

From: jhart@ProInsure.co.uk
Subject: Look at this ....!

What should Alice do?

Option 1: Open the email
Option 2: Delete the email

Answer: Delete the email. Company email is not for private use. But what would have happened if Alice had opened the email from her friend?

From: jhart@ProInsure.co.uk
To: alice.koh@BeInsured.com
Subject: Look at this ....!
Hi Alice
I know you'll love this! Just click on the link below for a great laugh!
http://www.globaljokes.lagos/laughoutloud.zip
Seeya!
J

What should Alice have done?

Option 1: Clicked on the link
Option 2: Deleted the email

Answer: Deleted the email. Emails such as this should never be opened. Mostly, infected emails will be picked up by corporate firewalls. But cyber criminals are forever and quickly coming up with new ways of getting through IT security. Clicking on the link could have disastrous consequences. The email should be deleted, or better still sent to IT security [DN

But what would have happened if Alice had clicked on the link? The zip file downloads. Alice laughs at the joke, clutching her sides!

What was the harm in that then?

Option 1: All perfectly innocent and a laugh to break up the day?
Option 2: Harmful

Answer: Harmful. A fraudster has infected Alice's PC with a 'trojan horse'. This means that he can track every key stroke she makes as she uses her keyboard, including her system logon and password.

Unsolicited emails, even those from friends that contain links to websites or zip file attachments should be treated with extreme caution. Zip files may well contain viruses and trojan horses which track every keystroke you subsequently make on your computer keyboard, including logons, passwords, bank account numbers, credit card details, and internet shopping security questions. Fraudsters who infect PCs in this way quickly have everything they need to raid bank accounts and hijack identities. Those bank accounts and identities could as easily be your customers', such as Emma's, or if you open unsolicited emails at home, your own.

5. Stranger in the pub

As you further investigate Emma's losses resulting from financial crime and the hijacking of her identity by a fraudster, you learn that a number of people from the company which provides her insurance meet every week after work at the pub near the office.

"We all know what it's like! The phone hasn't stopped ringing. You've spoken with dozens of people. There's the admin to finish. Everyone wants something from you all day and every day. Deadlines to meet. Pressure, pressure ... pressure! In our team, there's a real camaraderie! I suppose it's a bit like the Dunkirk spirit! We all work together, support each other, look after eachother. And when the day is done, we celebrate together. In the pub. The one just over the road from the office. You know the one! You'll find at least some of us there after work most nights. That particular Thursday night? It's a while back now! But I think there were just four of us there that night: There was Jane, Graham, Alice, and me. John's the name. I can tell you what I remember, but you'd have to ask the others what they recall."

Find out what John, Jane, Graham and Alice remembers:

What John remembers
"We don't talk about work all the evening, you know, but it's usually how things start out. We'll talk a little about things that irritated or frustrated us during the day, or perhaps about things that made us laugh! Jane was telling us she was working on a really "hush hush" project that she wasn't supposed to talk about, even to us! A big city firm has invited us to bid for a really important contract. Something to do with processing insurance claims for several hundred thousand customers. If we get it right, we have the chance of winning a really huge contract. Jane was very excited about working on the team. Alice had been talking about how she had brightened up her workstation with some photographs of her cats. She's a real cat lover herself you know! Not my thing! Graham was getting fidgety because the following day was his month end and he had to get a whole lot of sensitive information electronically sent to another company. Somehow the conversation turned to how untidy the office has been over the last couple of days. Turns out that the confidential waste bins which are usually emptied by a contractor, haven't been emptied for about a week. I didn't take too much notice, but I think Jane seemed to know all about it!"

What Jane remembers
"I don't remember much about that night at all. Anyone who says they can remember is lying! We literally propped up the bar after work for hours! But now you come to mention it, of all things, there was some conversation about confidential waste. And yes, there was someone on a nearby table who seemed to be taking an interest! But I don't think anyone said anything that they shouldn't have said."

What Alice remembers
"Well, we were talking about cats for a while. Then things went a little blurred! I do remember a guy from the next table came over and joined us. Yes, now I think of it, he worked for that company that collects our confidential waste. You know the one! They unlock the bins, put confidential reports and papers into a sack and take them off somewhere for shredding. ConfidiShred! That's the one! Don't see the point myself. Why it can't just be recycled I'll never know."

What Graham remembers
"I remember drinking. The rest is a bit of a haze. Jane? I don't think she was there. Or maybe she was. Yes! You're right, I did speak to her. She was telling us about a proposal

she was working on. Some big city company wanting to buy something from us and she was on the team putting in the proposal. Hush hush? I don't remember her saying that, no! But I don't imagine anyone would have remembered anyway - we were so tanked up! Confidential waste? That was me. The usual guy, Colin, is off sick. That's why ours hasn't been collected for a few days. Dreadful. It's all over-flowing everywhere. We've taken just to sticking confidential reports into the bin! Not ideal. The next table? Empty, I think. ConfidiShred? Yes that's the company that collects the confidential waste for us; that's it, Colin works for them. No! No! There wasn't anyone in the pub that I recognised from ConfidiShred."

Criminals are known to target pubs and clubs, especially those near call centres and the offices of large corporates. They know that after a few drinks people loosen up, talk louder and are likely to be less careful about what they say. They may just sit in the background listening. Or may expertly involve themselves in your conversation. They come across as very sociable and seem to fit into the crowd quickly and easily. And of course, as the evening wears on, people become less guarded in what they say. The information criminals can glean from pub conversations are rich pickings for them. By eavesdropping in pubs, fraudsters may acquire information which enables them to access:

- Your office
- Personal information to commit fraud
- Data sources for bank and savings account

Careless talk can cost you:

- Money
- Your job
- Your passport or driving license
- Your whole identity
- Always beware what you say when you are out and about in public places.

Now think for a moment about what you hear people say and see people do in public places; in bars, in clubs, in coffee shops, in train stations, on trains, on the 'phone in supermarkets, and so on. Which of the following have you seen or heard?

Someone working on a laptop on a train who leaves it unattended when they go to the buffet
Never leave laptops, USB sticks, DVDs and other work related material unattended when on a train, even for just a moment.

Someone on a mobile 'phone in a coffee shop talking loudly about a business meeting they have just finished or are about to go into
Mobile 'phones do strange things to us! When we speak into them, we forget ourselves and where we are. Never have conversations about business in public places which could reveal anything about who you work for, what you do, who your clients are.

Someone engaged in a very personal conversation with a friend about their partner

Others might do it, but conversations like these can lead to serious consequences. The stranger on the next table might be a long lost relative who reports back the conversation to the partner, i.e. the subject of the conversation.

Someone leaving a wallet on a table in a pub whilst concentrating on something else
If you have never seen this before, look harder!! Look around the office, look around pubs and coffee shops, look around cafes and restaurants. It may not be a wallet left lying around, but it could be a smartphone which could be worse. A smartphone might give a criminal everything he needs to access your hard-earned cash. Never leave anything unattended or out of sight in public places.

Someone getting off a train having left a file or folder on the seat beside them
There have been plenty of news reports in the last two years of very senior, highly intelligent people leaving sensitive files and folders on trains which have then ended up in the newsrooms of national television channels. Make sure you have everything with you at all times.

Someone muttering their logon and password as they use their laptop in a coffee shop
Strangely, people do talk to themselves whilst they are working. Whilst they work, they are so lost in what they are doing that they forget themselves and behaviour that is acceptable in private becomes the norm in public too. Never reveal your logon or password to anyone!

6. Graham's story

As part of an ongoing investigation into Emma's unfortunate experience as a victim of financial crime, you have learned that Graham was at his desk, busy at his computer. He had a deadline to meet; an important report had to be completed by mid-afternoon and there had been a whole host of distractions earlier in the day. Now, though, he seemed to be making progress. You have learned that most of the work-stations around Graham were empty. His colleagues were either out of the office or in meetings in other parts of the building. Graham tells you that from the corner of his eye, he saw a figure wandering around the office. He looked up from his work in the direction of the figure. A stranger. A man in a boiler-suit. A man who was carrying a seemingly heavy sack around with him. At the time, Graham was asked to produce a statement of what he did when he noticed the stranger. In addition, the investigation has uncovered some Closed Circuit Television material (CCTV) captured from around the office. As part of your own investigation, you can:

Option 1: read an extract from Graham's statement
Option 2: view images from the CCTV
Option 3: find out what was in the confidential waste bins that "The man" had come to take away.

Extract from Graham's statement
"I left my seat and moved closer to the stranger. I could see some kind of corporate logo across the breast pocket of his boiler suit and underneath it, the word ConfidiShred Ltd. I recognised the name of the company. ConfidiShred is the firm that regularly collects all our confidential waste, (sensitive information, confidential reports, customer information, and the like), from the office complex and removes it for secure shredding. I've worked here long enough, think I know most people who work in the office and I would recognise most visitors, but this stranger was completely unknown me. I approached the stranger and mentioned that I hadn't seen him before. He told me he was just covering for Colin who was off sick today. Of course, I knew Colin. Colin had been coming to the office for years to collect the confidential waste. I asked the stranger whether he had any identification. 'Yes,' he said. 'Here's my ID.' But the ID the stranger showed me was from his own company. I could see his company's logo, a photograph of the stranger, his name, which was apparently "The man Smith" and his employee reference number. The fact that he knew Colin made me think he probably had authority to be here. And he was doing what Colin normally did."

Images from the CCTV
As you investigate the fraud committed against Emma, you have now been given access to some images captured from the closed circuit television cameras positioned around the office. There are six images.

1. **The man standing over unattended desk**

Leaving personal possessions and company sensitive information lying around unattended on or by desks is risky. You may be able to trust your colleagues, but they are not the only people to have authorised access to the building.

2. **Confidential waste container**

Confidential waste is for shredding, not for prying eyes.

3. **Photography**

To take photographs around our buildings requires special permission. Always challenge anyone who is taking photographs around our offices. The man may well be relying on

gathering the names and contact details of people who might inadvertently provide him with more information that will be useful to him in the future.

4. **Waste bins**

The man now has Emma's credit card details which John had earlier noted on a scrap of paper and left lying in the bin.

5. **Tailgating**

You may be in a hurry, but as you enter the office, always check that the door has securely closed behind you. You don't want to be the one who lets in an intruder!

6. **Documents and files**

Leaving anything lying around on desks unattended is risky.

What was in the confidential waste bin?

As you delve further into how Emma became a victim of financial crime, you discover that auditors have recently emptied a random sample of confidential waste bins and sifted through their contents in order to produce an audit report. You now have an extract of this audit report which lists examples of the items they found. From the list shown below, which do you believe to be items of a confidential or non-confidential nature?

1. **A draft letter to Emma confirming details of her life insurance policy**

Confidential

Details of life insurance could well include the insured's date of birth, policy number, salary, the benefits the insured will receive in the event there is a claim, the insured's bank sort code and account number if paying by direct debit. This is confidential information.

2. **A job description for a job that was filled by an outside candidate six months ago**

Non- Confidential

The job was filled by a candidate not already an employee of the company. The job must therefore have been advertised in some way, e.g. in newspapers, on web sites. This is not confidential information.

3. **A copy of a contract between the company and a supplier**

Confidential

Contracts are private between the company and its suppliers and must therefore be regarded as confidential

4. **The company's mission statement**

Non-Confidential

Mission statements are generally published; they are often regarded as a means of assuring customers of the company's purpose. This document is non-confidential

5. **An out of date copy of the company's employee handbook**

Confidential

This is at least company confidential – it gives a lot of policy information. If in doubt, always put it in the confidential waste bin.

6. **A letter to a customer confirming details of the transfer of their pension from one pension provider to another**

Confidential
This will contain details of the policy holder's policy number, amount transferred from one provider to another, and possibly even the policy holder's national insurance number. This is confidential information.

7. **A manager's interview notes of four candidates for a recently advertised job**

Confidential
Individuals have a legal right to see the notes made about them at interview. They should therefore not be disposed of at all unless they have first been scanned. Since they are about specific individuals, they must be regarded as confidential

8. **A recent press release sent by the communications department to newspapers and professional journals about a new product**

Non-Confidential
Press releases that have already been sent to newspapers, professional journals and other media about new products are not regarded as confidential. The more people who see them, the better! The marketing department's annual budget X Departmental budgets are the business of the company alone, and are not for any other person or organisation. They are therefore regarded as confidential.

9. **Job applications from 75 applicants for a recently advertised job**

Confidential
Job applications contain personal information about the applicants. They must therefore be regarded as confidential

10. **Recent but as yet unpublished research by the company**

Confidential
If the company has undertaken research and has produced a report which has not yet been published, it could well be disadvantaged if competitors saw the report prior to publication. Any unpublished research material must be regarded as confidential

11. **An analysis of all sales made over the last month**

Confidential
Companies must provide certain financial information in their annual accounts. Sales made during a month do not need to be published. It must be regarded as confidential

12. **Screen shots from the company's web site**

Non-Confidential
If the web site can be viewed by the world at large, these screen shots are not confidential. However, if the web site is being designed or updated, and these are screen shots of a site that has yet to be made available to the outside world, these screen shots are likely to be confidential

13. **A medical report from a doctor about a customer who has applied for permanent health insurance**

Confidential
Any medical report about any individual is to be regarded as confidential

14. **A signed and dated copy of a confidentiality agreement between the company and a supplier**

Confidential
Companies often require suppliers and partners to sign confidentiality agreements to ensure that the matters they discuss and the services provided and bought are kept entirely confidential.

15. **Records of employees who left the company more than five years ago**

Confidential
However long ago an employee may have left the company, employee records must always be regarded as confidential

16. **Marketing materials such as leaflets, brochures and other printed matter to help sell the company's products**

Non-Confidential
Marketing materials are produced to sell products and services and to enhance the reputation of the company. These are not regarded as confidential.

What should Graham do?

Option 1: Ask to see a visitor's badge or contractor's badge
Option 2: Escort the man to reception
Option 3: Phone reception

Answer:
Telephoning reception immediately is the preferred option. This ensures that everyone who needs to be is alerted to the fact there is a possible intruder to the building and ensuring that the intruder can be quickly found.

People fall victim to financial crime because of a series of seemingly unconnected incidents. Confidential documents that are no longer required are safe only if they are in the confidential waste bins. If an unauthorised person gained access to the building and remained unchallenged, they would put the staff, clients and the company at risk. They may access confidential information about an individual or the company and they could remove valuable assets or people's valuables. Whenever you enter or leave the office, always check that the door has closed securely behind you and never allow people to follow you into the office. We all have a responsibility to protect people like Emma, and to protect our colleagues too!

Think about people who come into the office aside from regular colleagues.

- New joiners
- Visitors
- Customers

- Contractors

You may have seen them before or they may be complete strangers. They should ALL have security ID badges displayed. When you are away from your desk always lock down your screen and never leave possessions or company information lying around. That way, you can be more confident that we are better protecting Emma's personal information and the personal information of all our customers and colleagues.

What to protect

Graham is responsible for maintaining a database of thousands of employees to ensure salaries are paid and tax, insurance and any pension contributions are deducted. Sometimes, when people like Emma advise him of a change to their bank account details, or pension contributions, or when he receives a communication about tax, he has to make changes to employee details. These can include tax codes, bank account details, pension contributions and so on.

Look at the details and information on this employee form. Which of these should Emma be worried about falling into the hands of a frauster?

1. **Employee name**

Emma might not be worried about her name. After all, it is probably in the public domain through the electoral register. Anyone can get hold of names and addresses. Emma might still want to protect her name. After all, any fraudster needs their victims' names in order to commit financial crime. And if Graham's database goes astray, anyone could call her at work knowing precisely how to get hold of her.

2. **Job / Position**

Why should Emma mind if people know what her job is or who she works for? She has probably told many people in any case! But organised criminals target particular types of people and a job title might just put Emma in their sights. Even if she is not a target, imagine this scenario: You receive a call at work regarding confidential work for the chief executive and you may be able to help with some crucial information. You provide information that in normal circumstances you would probably not, and unwittingly provide the names of colleagues who might be able to add more. Now a potential fraudster has a growing body of knowledge about the company and an expanding list of people who work in it.

3. **Department**

If you were Emma, you might not be concerned about the name of the department you work for falling into a fraudster's hands. But fraudsters are adept at building pictures. Once they know your name, the company you work for and the department you work in, they can set about identifying the names of your manager and colleagues and their personal details too. As they build their picture, they find out ever increasing amounts of information about the company, and their potential list of victims grows.

4. **Address**

Emma might not be worried about her home address. It is, after all, on the electoral register. But if a fraudster wants to gain access to your bank account, your pension, your mortgage, your insurance, he will have to provide proof of who he is. He needs to know where you live.

If you are one of the many who do not yet shred your gas, electricity and phone bill, he may well have rifled through your bin last night and found what he was looking for. Gas bills, phone bills, electricity bills are typically used by many of us to prove our identity when we open bank accounts, set up pension arrangements, open savings accounts, etc.

5. **Home phone number**

Emma might not be worried about her telephone number. After all, it is probably in the telephone directory.

But how many times do you get calls, in the evenings, from people trying to sell something, or trying to get personal information as part of their market research? Most of them will be selling legitimate services. But the telephone is a key 'tool' used by fraudsters to persuade people to part with their credit card details - card number, issue date, expiry date and three digit security number from the back of the card - all the fraudster needs to use the card to shop online or make purchases by telephone.

6. **National insurance number**

Our national insurance numbers are unique reference numbers.
We are allocated these at the start of our lives and they stay with us throughout. They are used:

- by HM Revenue and Customs in any communications about income tax
- if we open an Individual Savings Account (ISA)
- when the Department of Work and Pensions communicate with us about our state pension entitlements
- by pension providers when we set up personal pensions or if we are a member of a company pension scheme
- by our employers and appear on every payslip, every P60 (the document we receive from our employer at the end of every tax year), and P45 (the document we receive from our employer when we leave their employment).

Protecting our national insurance numbers is crucial to protecting our identities and protecting our personal possessions.

7. **Pension policy reference number**

If you were Emma, you might just think this was a reference number.

But imagine this scenario: You have been working for thirty years since leaving school. You are considering retiring early and call your pension provider to find out what your pension is worth. You are shocked to learn that your pension is nowhere near the value you expected and you may not be able to take early retirement after all. You discover that a fraudster who had your full name, your full address and postcode, your date of birth, your national insurance number and your pension policy reference number managed to convince the pension provider he was you, and took 25% of your pension as a cash lump sum, getting it transferred to his own bank account.

8. **Salary, tax and pension contributions**

This is valuable information for a fraudster and Emma should take great care to protect it. With this information, a fraudster has an idea what Emma is worth in financial terms. He also has sufficient information to telephone her employer, pension provider or the tax office

pretending to be Emma and persuading the people he calls to part with further personal information that will help him raid her account and hijack her identity. Always protect this information, whether it is yours, or whether you are the guardians of it for others.

9. Bank account details

Like Emma, you might think that as your bank account details are on any cheque you may write out, it is not that sensitive. If fraudsters want to empty your bank account, like they emptied Emma's, they first need your bank account details! Always protect your bank account details!

Now let's see the challenge Graham faces as that point in the month arrives when he has to transfer information from the database to the outside company which processes employee salaries and produces the payslips.

Graham faces his nightmare scenario! The data is usually transferred, by Electronic Data Interchange, (EDI), a means of transferring data electronically securely and encrypted so that employees' personal information is secure. If Graham's data is not transferred today, thousands of people will be without payslips, and will not be paid on time! Graham has a monthly schedule: when he must run his final checks on the employee database and when he must transfer the data to an external company paid to calculate everyone's monthly pay and produce their payslips.

Given that amongst the employee data he needs to transfer is Emma's personal information including her updated bank details, if you were Graham, which of the following methods of transferring the data would you choose?

A. Hard copy (e.g. printed paper).

B. Soft copy (e.g. CD)

C. Attachment on email

A. If you choose this option, how will you send the hard copy?

1. Signed for post - This provides you with proof of posting and IF it arrives at its destination, a signature. It does not guarantee delivery. This is not an ideal method for sending sensitive personal information.Try another option.

2. Ordinary post - This provides no proof of posting or proof of delivery. Never put sensitive personal information in the ordinary post! Try another option.

3. Courier - Good choice. This provides proof of despatch and, as long as it does arrive, proof it has.

B. If you choose this option, how will you send the soft copy?

1. Signed-for post - This provides you with proof of posting and ***IF it arrives at its*** destination, a signature. It does not guarantee delivery. Try another option
2. Ordinary post - This provides no proof of posting or proof of delivery. Try another option
3. Courier - Good choice. This provides proof of despatch and proof it has arrived. Top Tips
    - Keep a log of the date and time of despatch
    - Note the name, company and address of recipient
    - Telephone the recipient to advise them of a couriered item
    - Ask the recipient to call you when they receive the despatch
    - Do not wait to hear from the courier firm for confirmation of receipt

Couriers have been known to have been robbed or involved in accidents which could leave your information vulnerable.

C. If you choose this option, how will you transfer the data as an attachment on the email?

1. Encrypted email – If you send an email with or without an attachment containing personal or confidential information, always encrypt it. Never assume that password protecting a Word, Excel document or any file type is good enough – these passwords can be easily hacked.
2. Unencrypted email - Never assume that password protecting a Word, Excel document or any file type is good enough – these passwords can be easily hacked.

CAPITA
LEARNING & DEVELOPMENT

7. Jane's story

A potential client has invited the organisation to bid for a contract to process insurance claims. It's a five year contract with the potential to create hundreds of jobs and lead to more business. Jane is helping to prepare the bid. To help prepare the bid, the client will send some confidential information. But first Jane must sign a confidentiality agreement on behalf of her organisation not to disclose any information about the client or the bid. Jane signs the agreement and returns it to the client. Just as she is leaving the office, the confidential documents arrive from the client. She likes to think that because of Emma's experience, she now takes better care of personal and confidential information. Yet, she decides to take them home to read overnight.

At the station, late for the train, Jane puts her bag on the floor by her feet to take some cash from her purse to buy a ticket. This is one of the most common ways laptops and bags are stolen. Others are lost in pubs, clubs, coffee shops and hotel reception areas.

Having missed her train, Jane has forty minutes to wait. Jane goes to a coffee shop and takes out the confidential documents to get started. She does not notice someone nearby taking a close interest. Can he be noting something down?

Having caught the train, Jane arrives back at her home station where she has left her car. She puts her bag on the seat of the car. On the way home she stops at the local supermarket to buy groceries. Criminals are known to lurk in car parks with the primary purpose of stealing laptops and valuables. Jane has been seen leaving her bag on the seat of her car in full view. This could be an opportunity too good to miss.

As Jane is going round the supermarket she is on the phone talking to a colleague: *"Yes, ProInsure want us to bid for a five year contract to process client insurance claims. Their staff don't know about this, so it's strictly hush-hush."* Unbeknown to Jane, the person behind her in the supermarket is listening to her conversation intently and noting something down.

Having arrived home, Jane has left the laptop and documents on her desk and is making a drink in the kitchen. Meanwhile, Jane's cleaner is taking particular interest in the laptop. Later, Jane went out for the evening. When she got back she learned that burglars had broken into her house through an upstairs window. Unfortunately, she had not locked away her laptop or the confidential files and had left them on her desk. They are nowhere to be found!

A couple of months later, following fall-out from the theft, the national newspaper headlines reported:

"JOBS AT RISK AT MAJOR INSURANCE COMPANY AS CLAIMS PROCESS CONTRACTED OUT"

Consequences

What potential damage could be done as a result of Jane's lapse and the loss of the laptop and confidential documents?

1. Jane could be reprimanded by her manager

Yes
She has signed a confidentiality agreement and should never have taken out such sensitive documents from the office.

2. Jane could lose her job

Yes
She could be subject to disciplinary action which may in turn lead to her dismissal and / or prosecution, depending on the circumstances.

3. The client could remove Jane's company from its list of possible suppliers

Yes
Jane and her colleagues lose out not just on this particular contract but on all possible future contracts. Clients do not take kindly to confidences being broken, even if they are by accident. They expect better from the suppliers they hire to work for them. This could be very costly for Jane's company.

4. If Jane's company already has an existing contract with the client, the client might terminate it

Yes
This is quite possible. Jane's action sends strong signals to the client that her company cannot be trusted and is therefore not a supplier they would want to work with.

5. Redundancies could arise as a result of any lost contract

Yes
It is not only Jane whose future has been put at risk by this lapse on her part. Others could easily lose their jobs if existing contracts are cancelled. When companies lose their clients' confidential information, existing and future business is jeopardised.

6. Jane will be thanked by her manager for being conscientious enough to take her work home

No
Whilst Jane's intention may have been praiseworthy, nothing can excuse her behaviour, or the loss of the documents.

7. Jane's company's business reputation will be tarnished

Yes
Whether Jane's lapse is reported in the press or not, this is a very small world! Her client's bad experience will be repeated many times to other potential clients and word will quickly get about that Jane's company is not to be trusted.

8. Jane will describe her experiences as part of a new information security awareness programme

No
Possible, though unlikely! Whilst it is always useful to hear of the experience of others' lapses that result in information loss and breach of confidentiality, Jane is hardly an example to be paraded.

9. Jane's personal reputation will be tarnished

Yes
Jane can expect her lapse to be recorded on her employee record. She may well be disciplined. She may well lose her job. Her trustworthiness will be questioned in thefuture.

Conclusion

Jane could not be held responsible for the burglary from her house. However, she is wholly responsible for:

- Removing confidential documents from a safe and secure office environment
- Leaving documents unsecured at home where a cleaner could read them
- Leaving the house unattended without securing the documents

Confidentiality means confidential. Our clients, whether they are people like Emma, or corporate clients who have customers of their own like Emma have the right to expect us to treat their information with the respect it deserves and for us to honour the trust they put in us.

8. Sarah's story

As you work through the investigations into Emma's financial losses and the hijacking of her identity, you discover that she made a call to the council tax office, querying her payments. It emerges that she believed there was an error and that incorrect amounts were being collected by direct debit. On behalf of the council, Sarah took Emma's call. The call was recorded, so you now have access to the transcript. You will notice Sarah says some things that give cause for concern.

Sarah: How can I help you?

Emma: I have a query about my council tax. You should be collecting payments by direct debit, but I can't see any payments for the last four months. I can't access my records. Can you help?

Sarah: Let me see what I can do. First, can I take your name please?

Emma: It's Mullen. Emma Mullen.

Sarah: Is that one 'l' or two?

Emma: Two. M.U.L.L.E.N

Sarah: I can't find anything here. Could it be spelled with one 'l' ?

Emma: Yes, try it with one then.

Sarah: OK. I've found the record. For security purposes, I just need to ask you a couple of questions. Could you confirm your postcode please?

Emma: TW1 8PZ

Sarah: Thank you. That's fine. Can you give me your date of birth please?

Emma: Yes, it's May 19th, 1972.

Sarah: Thanks. Can you tell me the name of the first school you attended?

Emma: It was Twickenham Manor Primary School.

Sarah: Ah! I'm afraid that's not the information that we have down here.

Emma: Oh no, that's not right! My parents moved when we were very young. Now what was the name of the school ...?

Question: At this point, what would you do in Sarah's position?

1. **End the call and suggest Emma call back when she has all her information to hand**

If the caller really is Emma, she can always call back when she has the information. The process may vary for different businesses, however recommended good practice would be to request that the customer write in with their request. But if there is any reason to be

suspicious, then the matter is worth reporting in case the caller tries calling again in the hope that a more amenable colleague will give information away.

2. **Report your suspicions to a manager**

If there is a possibility that the caller is not really Emma Mullen, then you must report your suspicions immediately. The caller, having not managed to get anywhere with this call might dial again in the hope of speaking with more amenable colleague. Therefore, such incidents should be recorded on the system and reported.

Now find out what Sarah actually did.

Sarah: I'm sorry. I do need you to correctly answer the security questions in order to help you with your problem.

Emma: Oh. It's the same school as my husband went to.

Sarah: I can't really help you. Can you ask your husband?

Emma: Well, he's away for a few days and out of telephone contact.

Sarah: I'm so sorry. I can't help you.

Emma: Is there anything you can do?

Sarah: I can ask you another security question if that will help.

Emma: Thank you. It's really silly. I know it was the same school my husband went to.

Sarah: Well, if you can just give me the password on the account please.

Emma: Patsy

Sarah: No, I'm sorry that's not correct.

Emma: Gareth?

Sarah: No, that's still not correct.

Emma: Isn't there anything else you can do to help me?

Sarah: There is a reminder question registered here. The question is: what is the name of your dog?

Emma: Ferago

Sarah: That's right. Now, let's have a look at your records. Ok, well your payments are up to date.

Emma: I don't see how that's possible! There's nothing on my bank statements.

Sarah: Well, everything is fine, I can assure you.

Emma: I wonder whether it's coming out of the correct bank account. What details do you have on record for me?

Sarah: Well, the sort code is 10-01-15 and the account number is 06324185.

Emma: That's the right account. I'd better talk to my bank about it. Thanks for your help.

Sarah: Is there anything else I can help with?

Emma: No thanks. You've been a real help.

Question: How did Sarah handle the call?

During the course of the call, Sarah said and did some things that raise some concerns. Which of the following would concern you?

Sarah should not ask Emma if her surname is spelled with just one 'L'.
This could be cause for concern. Emma previously said her surname was spelt with two 'L's'.

Sarah should not ask Emma the 'reminder' question, i.e. the name of her pet.
This is not cause for concern. Where reminder questions are a part of security questions, there is no reason why they should not be asked in order to verify the identity of the caller.

Sarah should not give out bank sort codes or account numbers held on file.
This is cause for concern. Providing this information to the caller could have serious consequences. If the caller is not Emma, an unauthorised person, possibly a fraudster, now has Emma's bank account details. This information should only be confirmed in writing to the address held on file.

Sarah is more concerned with asking the questions on her list than with determining the caller's identity.
This can be cause for concern. There is more to asking and getting correct answers from the caller to determining whether the caller really is who they say they are. Emma made a number of incorrect, indeed suspicious responses which Sarah should immediately have escalated.

Sarah should not ask Emma for her postcode.
This is not cause for concern. Post codes are often used to establish a caller's identity. It was perfectly reasonable of Sarah to ask this question.

Sarah should not ask for Emma's date of birth.
This is not cause for concern. Dates of birth are often used to establish a caller's identity. It was perfectly reasonable of Sarah to ask this question.

Sarah should not continue the call if Emma cannot provide the name of her first school.
This could be cause for concern. Emma's claim that she had moved when very young is just about plausible and could, possibly, be a reason why she initially incorrectly answered this question. However, she was subsequently unable to provide the name of her first school. It would have been better if Sarah had invited Emma to write in with her query and then have ended the call.

Conclusion

Although local procedures may vary, if security questions are answered incorrectly, the caller should be asked to write in with their query.

If the caller has answered a number of security questions incorrectly, details of the caller should be reported to a line manager. Anyone taking a call needs to be confident that the caller really is who they claim to be, and that they are entitled to have the information they are requesting, before any personal or company confidential information is disclosed. Never give out over the phone, bank details or sensitive data such as National Insurance numbers. If a customer wishes to have these details confirmed, they should be asked to write in.

9. Anonymous caller

Find out what happened to Emma when she took a call one night at home from someone from the council tax office she had never spoken to before. Not everyone works in call centres handling customer calls. Surely it's only people who work in call centres that have to be careful about identifying callers by asking security questions? Why should we worry about this at home when we take calls or work in a non-customer facing job?

Emma: Hello?

Caller: Ms Mullen?

Emma: Yes.

Caller: I'm from the council tax office. I'm calling about your council tax.

Emma: Yes.

Caller: I just need to ask you some security questions. Is that alright?

Emma: Yes.

Caller: Can you just confirm your full postcode, date of birth and password on your account, please?

Emma: TW1 8PZ; 19th May 1972; Ferago.

Caller: That's fine. Thank you. I'm sorry to tell you that somehow you have overpaid your council tax so far this year. The good news is that you are due a refund.

Emma: That's marvellous news! How much am I owed?

Caller: £379. We're sorry this has happened. We'll transfer the money into your bank account within the next three working days.

Emma: No problem.

Caller: Can you just confirm your bank details for me? Your sort code and then your account number.

Emma: Of course. The sort code is 10-01-15 and the account number is 06324185.

Caller: Thank you for your bank details. The refund is on its way

Never give out personal information, especially bank or credit card details to unsolicited callers.

This is what Emma should have done:

Emma: I'm really uncomfortable with giving out that information over the phone.

Caller: I'm sorry, Ms Mullen. If you can't answer the security questions, I can't discuss your council tax with you.

Emma: Alright. I'll call the council tax office myself tomorrow.

Caller: Let me give you a number to call.

Emma: No need. I have the number on my council tax bill. I'll call that.

Conclusion
Whether we work in call centres, deal directly with customers or suppliers, or are simply answering the phone at home, it is vital to check the identity of the person who is calling you. Financial crime is committed by people who are expert at extracting information from us. They sound as if they have legitimate business with us; they gain our confidence; they sound as if they are speaking with authority. They often sound as if they are officials for some organisation or other we might expect to be dealing with.

- Never give personal information over the phone without checking who they are and that they have the right to have that information.

- If you take a call from someone wanting you to confirm security information, only give partial details for each.

- If they are still dissatisfied, make a note of their name, and call their organisation on a number from an independent source, (e.g. the internet, a telephone directory).

- If they really are who they say they are, they will have enough to be confident you are the person they mean to speak with.

10. In the coffee shop

As you follow Emma's trail, you learn that she met a friend in a high street coffee shop, just after she realised there was a problem with her council tax payments. Sipping your coffee, like Emma, you may be tempted to use your smart phone to check your bank statement online. But be mindful of some of the risks:

Advertising free wi-fi connection

Wi-fi connections in coffee shops and other public places are not secure. This means that anyone connected through such a public wi-fi connection can gain access to what you access, including your bank statement. Never use free wi-fi connections to look at personal information.

Discussing bank details

Beware of exchanging personal information such as bank details in public places. It may not seem that the information you are giving is particularly confidential or could leave you at risk, but a stranger, also logged into your account on an unencrypted wi-fi, may now have everything needed to empty your bank account.

A nearby stranger, straining to listen

Watch out for people around you who may be listening out for your personal information.

Logon details written down

Be aware of user names and passwords noted on pieces of paper. Any passerby can now see your bank account logon and password. Unless you change your logon and password immediately, anyone looking over your shoulder can access your account from a computer at their leisure.

A nearby stranger using a laptop

In public places such as coffee shops, cyber criminals use laptops and easy-to-access software to discover who is using unsecured wi-fi connections. Once they find you, whether you are using a smart phone or a laptop, the information you access, they too can access.

11. Summary

In this module, you have discovered that Emma may have fallen victim to financial crime and identity theft because the many people she trusted in the organisations providing a service to her failed to carefully protect her personal information. When we disclose our personal information to organisations that serve us, we have the right to expect they will preserve its confidentiality. Similarly, when we are entrusted with the personal information of our clients and their customers, we have an obligation to protect it.

To protect personal information, whether your customers', your colleagues, or your own, remember to follow these guidelines:

Documents
Shred any documents that contain personal or confidential information.

Personal information
Never write down personal information on jotters or pads that can be seen by others.

Screensaver
Ensure your screensaver is enabled and that it is strongly password protected.

Confidential files
Lock away any confidential files or personal information before leaving your desk, whatever time of day and not just at night.

Laptops
If you use a laptop in public places, use a privacy screen.

Removable media
If you need to copy customer data onto removable media (e.g. CDs, DVDs, USB memory sticks etc), you must not do so without the express written permission of the customer.

Where data is personal or confidential, it must at a minimum be encrypted (password protecting it as well is desirable), and the relevant passwords provided to the recipient in a different way. So, for example, if the CD is being sent by secure courier, the password could be sent by email. Ensure that any passwords used are complex i.e. made up of a combination of upper and lower case letters, numbers and special characters (such as !"£$) if possible, and make sure it is at least 8 characters long.

Public Wi-Fi
Never use public access wi-fi connections such as those found in coffee shops, pubs, railway stations, hotels, etc to access sensitive or confidential information, as you never know who may be monitoring your communications.

Home working
Be aware, if you work from home, of the need to securely lock away laptops and company information.

Public places
If you are in a public place, remember that eavesdroppers can hear you when you are speaking on your mobile, or talking with colleagues.

Company systems

Only use company equipment (e.g. desktops, laptops and Blackberries) to access company systems; never use your own or other a third party's equipment to access company systems without written permission from Group Security.

Tailgating
When entering the office, watch the door close behind you so there is no risk that unauthorised people gain access.

Out and about
If you must take company equipment such as laptops outside the office, or other confidential files, always keep it with you. If you are transporting it, remember to lock it in the boot from the start of the journey.

Verification
Do not disclose personal information unless you have verified that the person requesting it not only has an entitlement but also a need to have it.

For further information, see the Group Information Security Policies and Do's and Don'ts, on Capita Connections.

If you have any questions / suspicions on this topic, please contact

groupsecurity@capita.co.uk

If you want more information about protecting yourself, please refer to the following websites:

http://www.aboutidentitytheft.co.uk

https://www.identitytheft.org.uk

http://www.banksafeonline.org.uk