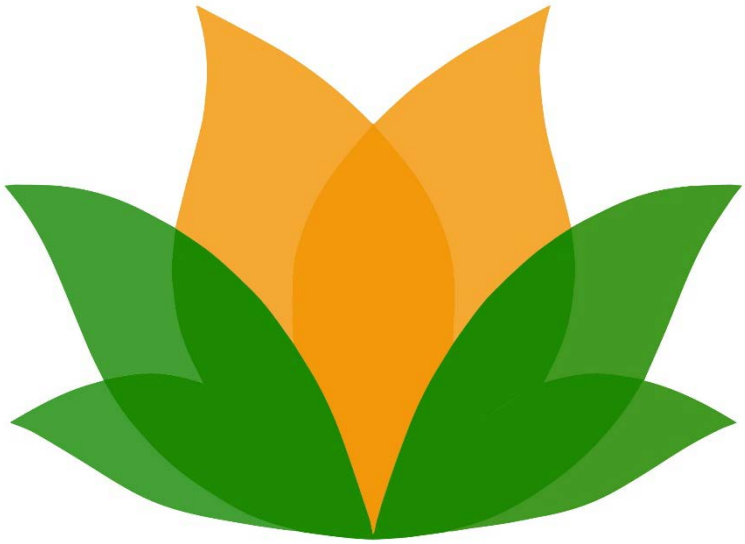

Fraud Prevention & Security Guidelines

November 2016

FLEUR TELECOM

Fraud Prevention & Security Guidelines

Contents

1. Introduction

With the rise of technology and the connected world at our finger tips, it's easier than ever to communicate with friends and family around the world.

We can have goods delivered within the hour, track our fitness using wearable tech, and even program our heating to come on so the house is toasty warm when we arrive home.

However, there is also a downside to the convenience the technology provides, which is **cybercrime**. Fraudsters (often referred to as 'scammers') are using this technology to hack devices and commit fraud.

The purpose of this document is to provide Fleur customers with information on fraud prevention and how to avoid becoming a victim of cybercrime. The guide aims specifically to provide an understanding of the following:

1. Examples of the different types of cybercrime and the jargon used
2. Tips for preventing fraud
3. Known methods used by the fraudsters
4. What to do if you have been contacted by a fraudster or fallen victim to a scam
5. Tips for safe internet browsing

2. Overview

The section below aims to provide an understanding of the different types of cybercrime.

2.1 What is Cybercrime?

Modern life is driven by technology. This brings with it all the benefits of the internet, and the convenience of managing our lives using technology.

However, this convenience also has its risks. With the rise of technology, it is not uncommon for our personal details to be stored on a computer, device or online.

There are individuals who see it as a personal challenge to 'break into' or 'hack' into our personal details stored online. These 'hackers' look to gain access to banking details, passwords and account recovery information which they can use to make financial gain at the expense of innocent victims.

Fraud prevention is an increasing priority for all of us in society.

Companies across all sectors are also looking at better ways to improve the security of their systems. Fleur is no different. We conduct regular and thorough security checks of our systems to ensure we have the necessary protections in place to keep records safe and secure.

2.2 How is Cybercrime Committed?

Cybercrime or fraud is committed in a number of different ways. The following are some common examples of how the fraudsters operate:

Through your Computer

There are a number of methods a hacker can use to infiltrate a computer or talk someone into allowing access to a computer.

You may have heard about viruses, Trojans, malware and spam. Below are definitions of the jargon you may have come across:

Computer Virus

A virus is a malicious software code that spreads throughout computers and mobile devices as it is able to copy itself and is often transferred from device to device through file transfers and emails. Viruses come in different forms but will be designed to cause some form of damage to your computer or gain access to your information.

Malware

Malicious software, or malware, can infect computers through the opening of an attachment within an email or clicking on an infected email. Once it is on your computer, it can be used to monitor bank accounts, steal money, view your files and data, send emails in your name and even use your webcam to spy on you. Examples of malware include: adware, bots, rootkits, Trojan horses and worms.

Spyware

Spyware can implant itself on your computer via your broadband connection and is used to collect information without the owner's consent, such as details of sites visited and passwords. It can also slow your machine down, and alter programs and settings.

Ramsomware

Ransomware is software code such as CryptoLocker. Ransomware code is designed to lock down your computer, preventing you from opening any files, and rendering your computer useless. A ransom demand request may then be displayed on your computer screen. Even if you do pay the fee requested, there is no guarantee that your computer will be unlocked. Further monies may be demanded.

Tip: Perform regular back-ups of your documents and data to an external hard drive so that you can recover your information if necessary.

Tip: Avoid opening files attached to emails ending in .exe as these are executable files and will run potentially harmful programs on your computer.

Tip: Hover the mouse over the name of the sender in your inbox – their email address should pop up so you can see if it looks genuine before you open it. Only ever open emails from someone you know. If you are in any doubt, delete the email without opening it.

By Telephone

Hackers will sometimes call people randomly, pretending to be from a genuine company, and talk innocent people into divulging their records verbally. The fraudsters are skilled and very adept at sounding genuine, so we advise all of our customers to exercise caution when receiving an unexpected telephone call.

Fraudsters will also sometimes offer a telephone number for you to call back to verify they are genuine. Always use the main contact numbers for the company, or if in doubt, check their contact numbers on their website.

Another method linked with the telephone is the fraudster asks the customer to call the company back and they pretend to hang up. However, they then dupe the victim by staying on the line and answering the call as the official company.

Premium Numbers

There are some 'scams' where the fraudsters trick people into dialling or texting premium rate numbers, thereby earning the fraudsters high amounts of money through the numbers dialled or texted.

3. What can you do to prevent fraud?

Cybercrime is becoming more commonplace in everyday life across all aspects of industry, from banking to utilities, and we are all constantly reminded to be more vigilant in changing passwords and running virus checks.

Passwords

- Changing your passwords on a regular basis, whilst inconvenient, does provide some level of protection from hackers.
- Never use the same password more than once.
- Consider making your passwords at least 8-characters long with a mixture of letters (upper & lowercase); numbers and special characters (e.g. # ! % £).

Anti-Virus

- Install a suitable anti-virus on your devices and run regular virus checks.
- We recommend installing Fleur Security Suite, or other third party virus protection software.
- Fleur Security Suite is for Windows-based devices and includes Symantec Endpoint Protection against viruses. It comes free with all 12 month Fleur broadband contracts.

Never allow remote access to your computer

Fleur will **NEVER** request remote access to your computer.

If you receive a call or email from someone purporting to be from BT Openreach, TalkTalk or any other company, in relation to your broadband or telephone line service, please be vigilant and call us direct on 0333 320 4020 so we can confirm if this was a genuine call.

We recommend never letting a third party connect to your computer remotely. Using software sharing applications, fraudsters can gain access to all areas of your computer, and potentially online banking details, if you grant them access. Examples of sharing software applications are:

- TeamViewer
- Windows Remote Desktop
- Join.Me
- WebEx
- LogMeIn
- AnyDesk
- KingViewer
- AMMYY

None of these software packages are themselves malicious pieces of software, but they can be used by scammers for fraudulent activity.

Engineer Visits

Should a BT Openreach engineer visit your property, they will conduct tests using their own laptop and the router. An Openreach engineer will never request to use any customer/computer equipment.

Telephone Calls

Fraudsters don't restrict themselves to computer fraud. They have been known to make calls pretending to be from a genuine company. They are skilled at sounding plausible and often begin a conversation with a 'reason for the call' leading to further conversation. If you receive a call from any company which you were not expecting, we suggest the following steps:

1. Always exercise caution.
2. Ask for the person's name and the company they are calling from.
3. Ask them to confirm the job reference related to the call. Make a note of any 'job'; 'pin' 'ticket' or 'case' references they quote you and advise you will check them.
4. Never allow someone calling on the phone access to your computer remotely, no matter how persuasive they may appear.
5. Never provide your bank details.
6. If in doubt, please be vigilant, terminate the call and search online for the real telephone number of the organisation that purportedly called you. Calling the organisation back on their published number will allow you to verify if the call was genuine. Do not call back on the number the caller has given you.
7. If you do terminate the call, make sure **you have dropped the call correctly** and **keep the phone off the hook for at least five minutes** before you make any further calls. Alternatively, use a different phone, such as a mobile, to ensure the line is clear.
8. If you are asked to remain on the landline for a lengthy period of time, and/or are asked to switch off your mobile, you should be cautious. Scammers do this to prevent your bank from calling you to verify fraudulent transactions.

If you receive a call or email from someone purporting to be from Fleur Telecom, BT Openreach or TalkTalk, which you are not expecting, please be vigilant and call us direct on 0333 320 4020 so we can confirm if this was a genuine call. Fleur will always run through data protection details with you.

If the fraudsters continue to call you, please call us and speak to one of our agents about a service called **'Choose to Refuse'** where calls from certain numbers are blocked. This is a free service for customers who have received a fraudulent call which they have reported to us.

4. Common Fraud/Scam Scenarios

"Refunds" or "credits"

Refunds and credits are a common approach used by fraudsters to gain bank details over the phone or via a computer. Some phrases to be aware of:

"We would like to refund/credit the money you recently paid to us."

"We recently refunded too much money into your bank account and we need you to enter your bank details on this screen so that we can take back some of the money."

Fleur will never ask you to transfer money through services such as MoneyGram or Western Union. Fleur will also never ask for remote access to your computer or for your bank details. If you are in doubt, please be cautious and call us on 0333 320 4020.

"You have a fault" or "you recently had a fault"

Another known method is where fraudsters call customers who may have recently been visited by a BT Openreach engineer. The **fraudsters appear to provide details about the visit including what sounds like a plausible job reference number**.

These fraudsters will talk about **needing further tests or giving refunds/credits for loss of service**. Customers can believe this call is from a credible source and grant them access to their computer.

General computer or broadband faults

Fraudsters take other approaches which involve alleged computer or internet 'faults'.

We are aware of some customers being contacted by fraudsters claiming to be from BT Openreach; TalkTalk; Microsoft; Fleur and other reputable companies in response to a 'fault'.

The fraudsters do sound plausible and may try to start the conversation with some of the following sentences:

"We have received error messages from your computer and your PC has contracted viruses".

"We see that you have recently been experiencing slow broadband speeds and problems with your internet connection".

"We have noticed problems with your router".

If you receive a call or email from someone purporting to be from BT Openreach, TalkTalk or any other company, in relation to your broadband or telephone line service, please be vigilant and call us direct on 0333 320 4020.

Computer takeover

Another common scenario: **by allowing fraudsters access to your computer, they can change or add a sign-in password. They may demand money in exchange for the new password, and without the new password, it can be very difficult to recover your data and information stored on the device.** Even if you pay the money, there is no guarantee the fraudsters will give you the password, and they may demand further payments.

"We could not process your latest bill. Click here to update your billing details now" or "Click here to verify your account, or it will be suspended"

If you receive a call asking you to update your bank account details, you should hang up, wait five minutes to ensure the call has dropped, and call the company back on their official number. If you receive an email claiming your bank account details are out of date, and asking you to click on a link to update them, you should never click on these links.

- If you need to update your bank account details, or set up a direct debit, you can do this through Fleur MyAccount. Alternatively, you can call us on 0333 320 4020.
- We advise never clicking on links in emails described above. If you do, it is likely that the scammers will be able to obtain your personal details and banking information once entered on the next screen.
- Another good tip is to check the sender's email address. If you mouse over the sender's email address, you can check whether it looks legitimate or not. For example, we have received reports from several customers who transferred from TalkTalk that they are receiving such emails. Whilst TalkTalk's name can appear in the sender field, mousing over the sender's name will reveal an email address such as: yourbill.talktalk.sales.uk.ni4353657ngsgfiqpaq@gseqwqkalp.fr

Telephone Preference Service (TPS)

The TPS is a **free** service which allows UK consumers to opt out of receiving nuisance telemarketing phone calls.

It's been reported in the news that some fraudsters are cold calling consumers, posing as the TPS or companies with similar sounding names, and trying to trick people into paying to block nuisance calls.

The TPS is clear that the service is free to use and the organisation will never contact you to request payments or card details. Once you have registered with the TPS, you will never be required to update your registration (see www.tpsonline.org.uk/ for more information).

5. Steps to take if you've been affected by cybercrime

Please note down as much information about the incident as possible. Useful information to gather is:

- Date and time the incident occurred.
- How the fraudsters identified themselves (full name and organisation).
- Telephone number or email address they contacted you on.
- What they claimed was the purpose of the call or email,
  e.g. "I'm calling from X Company; our system shows you have been experiencing slow speeds."
- Any 'job' or 'pin' reference numbers they quoted to you.
- What other information the caller had, e.g. last bill amount, fault reference number.
- Did they gain access to your computer or device?
  If yes, which program did they use? For example, TeamViewer; Windows Remote Desktop; Join.Me; WebEx; LogMeIn; AnyDesk; KingViewer; AMMYY.
- Were you were asked to log into any other application? E.g. Webmail; PayPal; online banking.
- Did the screen go blank or black at any stage?
- General information such as accents; whether the caller was a native English speaker; the duration of the conversation.

If you have had money taken from your account, it is also useful to note down the following information:

- Did you disclose your card or bank account details?
- Amount of money you believe has been taken, if applicable.
- Name of your bank and how funds were transferred.
- Date and time the funds were transferred.
- Any details about the beneficiary, e.g. **recipient name; account number; sort code; bank name.**

What should you do next?

- **Report the incident.** If the fraud is related to any service provided to you by Fleur Telecom, please call us direct on 0333 320 4020.

- Our team will ask you a series of questions in relation to the incident so we can capture as much information as possible for the authorities.

- Our team will also advise you to contact **Action Fraud** to report details of the incident on 0300 123 2040 or online at www.actionfraud.police.uk. This is an organisation linked to the police who gather intelligence on all reported incidents of fraud. They provide excellent advice and we do recommend you speak to them.

- If you've been duped into calling or sending a text message to a premium rate number, you can complain to **Phonepay Plus**. This organisation polices companies that use premium rate numbers; it can fine companies and may be able to aid you with obtaining a refund (see www.phonepayplus.org.uk/ for more information).

- If the fraudsters have gained access onto your PC, you may want to consider taking the PC to a local computer shop to remove any malicious software, and give it a health check following the incident. If you are unsure, we would advise seeking advice locally.

- If bank details have been accessed, money has been taken or if you are unsure about both of these points, we also recommend speaking to your bank for their advice on protecting your account based on your unique circumstances.

6. General tips for safe internet browsing

- Use virus and firewall protection software, and run full-computer virus scans on a regular basis.

- Never use the same password on more than one system or for more than one account.

- Use passwords of at least 8-characters with a mixture of capital letters, lower case letters, numbers and special characters.

- Regularly change passwords.

- Ensure all software and programs are up to date.

- Only enter your personal details on secure websites which start with http**s**:// and have a padlock or key symbol on the webpage.

- Check privacy settings on your social media accounts so you only share information with a restricted number of people.

- Always log out of accounts and your computer once you've finished using them.

- Ensure you are using one of the latest operating systems. The most vulnerable computers are those running Windows XP as Microsoft has stopped providing XP support.

- Remain cautious at all times when browsing the internet and opening emails. If you don't know who the email is from and are not expecting it, be cautious and don't open it. You should be especially careful with any embedded links or attachments in such emails.