Fraud Prevention Advice

Your Fleur Telecom reference number: FB000000

Dear Sir or Madam,

With fraud becoming more apparent in everyday life for consumers and organisations, we are writing to make all of our customers aware of common fraud scenarios and how to stay one step ahead of the fraudsters with our **Fraud Prevention and Security Guidelines**.

Telephone fraud is increasing, with an average of **eight calls made every second**. These criminals often pretend to be from a trusted organisation such as a bank or financial organisation, charity, utility or computer company.

Scammers are becoming more sophisticated, using phrases that sound very plausible when it comes to the communications sector. Examples of **regularly used phrases** which are used as an introduction in an attempt to gain trust, as well as access to your computer and banking details are below:

- "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."
- "We see that you have recently been experiencing slow broadband speeds and problems with your internet connection."
- "We have received error messages from your computer and your PC has contracted viruses."
- "We have noticed problems with your router."
- "We will compensate you for the inconvenience of this call."

Please remember that your bill is sent to you by Fleur Telecom, not TalkTalk

In the last few weeks, we have received reports that our customers are receiving emails with a request to provide their bank details to settle a bill.

If you receive an email with one of the following requests, even if it appears to be in a TalkTalk branded template, **you should not click on the link contained in the email**, and should report it to us.

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

What can you do to avoid fraud?

Be vigilant and follow the basic steps:

1. Never share your personal details or passwords.
2. Do not allow access to your computer.
3. Ask the caller to verify their identity – what is their name and job title?
4. What job reference did they quote? Note it down as it is often made up.
5. Trust your instincts. If it does not feel right, tell the caller you will speak to Fleur Telecom and then terminate the call.
6. Ensure you have terminated the call; wait at least 5 minutes and call Fleur on 0333 320 4020.
7. Be cautious of clicking on links in unexpected emails. No matter how genuine the format seems, always think twice.

We strongly advise against allowing remote access to your computer as fraudsters can change or add a sign-in password. They may demand money for the new password, and without it, it can be very difficult to recover the device. There is no guarantee the fraudsters will give you the password, and they may demand further payments.

Fleur's fraud guide

We have created a guide which provides specific advice on what to do in the event you are scammed; how to prevent fraud; as well as safe internet browsing. The guide can be viewed by clicking the following link: **http://fleurtelecom.co.uk/wp-content/uploads/2016/11/Fraud-Prevention-and-Security-Guidelines.pdf.**

There is also a **dedicated website page** where you can find out more information: **www.fleurtelecom.co.uk/fraudadvice**, and learn how to report a scam: **www.fleurtelecom.co.uk/fraudadvice/reportascam/**.

We hope you find the guide and website information useful. If you would like any further details on the subjects covered, or to report a scam call or fraud incident to us, please call 0333 320 4020.

Yours sincerely,

Frank Chapman
Customer Operations Director