Online Security Information: Phishing

What is phishing?

Phishing is the name given to the practice of sending emails at random purporting to come from a genuine company operating on the Internet, in an attempt to trick customers of that company into disclosing information at a bogus website operated by fraudsters. These emails usually claim that it is necessary to "update" or "verify" your customer account information and they urge people to click on a link in the email which takes them to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes.

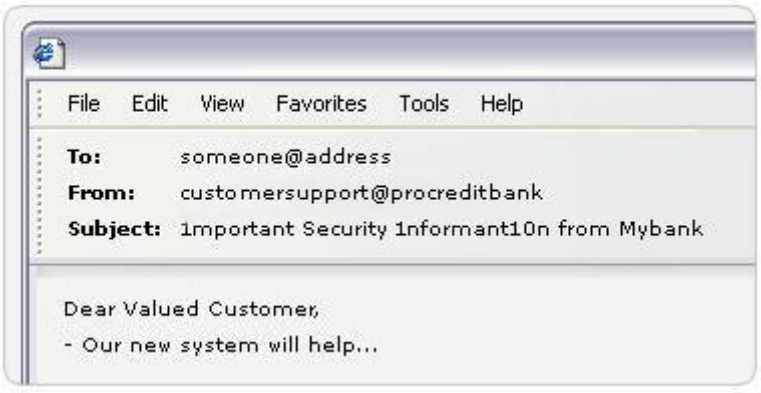
How can I avoid becoming a victim of phishing?

The key thing is to remain suspicious of all unsolicited or unexpected emails you receive, even if they appear to originate from a trusted source. The emails are sent out completely at random in the hope of reaching a live email address of a customer with an account at the bank being targeted.

Although ProCredit Bank may contact you by email, ProCredit Bank will never contact you by email to ask you to enter your password or any other sensitive information by clicking on a link and visiting a website. Stop to think about how your bank normally communicates with you and never disclose your full password or any personal information.

How to spot a phishing email

1 - Who is the email from?

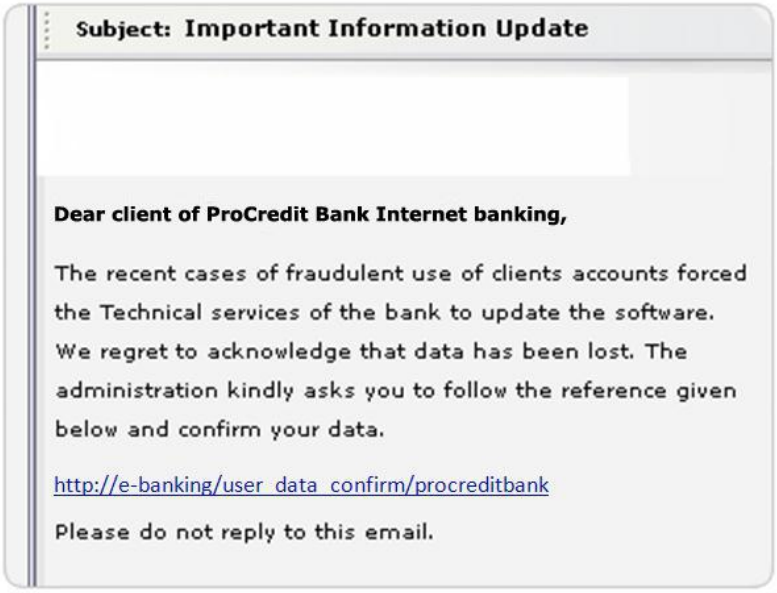


Phishing emails may look like they come from a real ProCredit Bank email address. Unfortunately due to the set-up of Internet email, it is a relatively simple matter for phishers to create a fake entry in the "From:" field.

The email address that appears in the "From:" field of an email is NOT a guarantee that it came from the person or organisation stated in the email address. These emails were not sent using the bank's own systems.

2 - Who is the email for?
The emails are sent out at random to bulk email lists and the fraudsters will almost certainly not know your real name or indeed anything else about you, and will address you in vague terms like "Dear Valued Customer".

3 - Take a closer look at the email - does it look "phishy"?


Subject: Important Information Update

Dear client of ProCredit Bank Internet banking,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge that data has been lost. The administration kindly asks you to follow the reference given below and confirm your data.

http://e-banking/user_data_confirm/procreditbank

Please do not reply to this email.

Example scam email

The first thing to remember is that banks will never write to you and ask you for your password or any other sensitive information by email. The message is also likely to contain odd "spe11ings" or cApitALs in the "Subject:" field (this is an attempt to get around spam filter software), as well as grammatical and spelling errors.

Never log on to your online banking account by clicking on a link in an email. **Always** open your web browser and type in ProCredit Bank's Internet banking website address yourself.

If you have any doubts about the validity of an email purporting to come from ProCredit Bank, please inform ProCredit Bank immediately by visiting your nearest branch, contacting your client adviser or phoning the following number (832) 2202222. You may also forward the suspicious email to the following email address **infosec@procreditbank.ge**

4 - Where's that hyperlink going to?
Unfortunately, it is all too easy to disguise a link's real destination, so that the displayed link and anything which shows up in the status bar of your email programme can be easily falsified.

How to spot a Phishing website

What's the site address?

If you visit a website after clicking on a link in an email, there are many ways of disguising the true location of a fake website in the address bar. The site address may start with the genuine site's domain name, but that is no guarantee that it leads to the real site. Other tricks include using numerical addresses, registering a similar address (such as www.mybank-verify.com), or even inserting a false address bar into the browser window. Many of the links from these pages may actually go to the genuine website, but don't be fooled.

You can confirm that you are on the official secure ProCredit Bank website by comparing the secure connection symbol

Internet Explorer 9

Internet Explorer 8

Firefox 4

You can check the **Security Certificate** of the ProCredit Bank website by clicking on the lock which appears on your browser.

Beware of fraudulent pop-up windows

Instead of displaying a completely fake website, the fraudsters may load the genuine website in the main browser window and then place their own fake pop-up window over most of it. If it is displayed in this manner, you will be able to see the address bar of the real website in the background, although any information you type into the pop-up window will be collected by the fraudsters for their own usage.

To access your online banking account, type the address into a new window yourself. The address of your real online banking website will start with “https” and will include a small padlock at the upper-right part of your browser window.