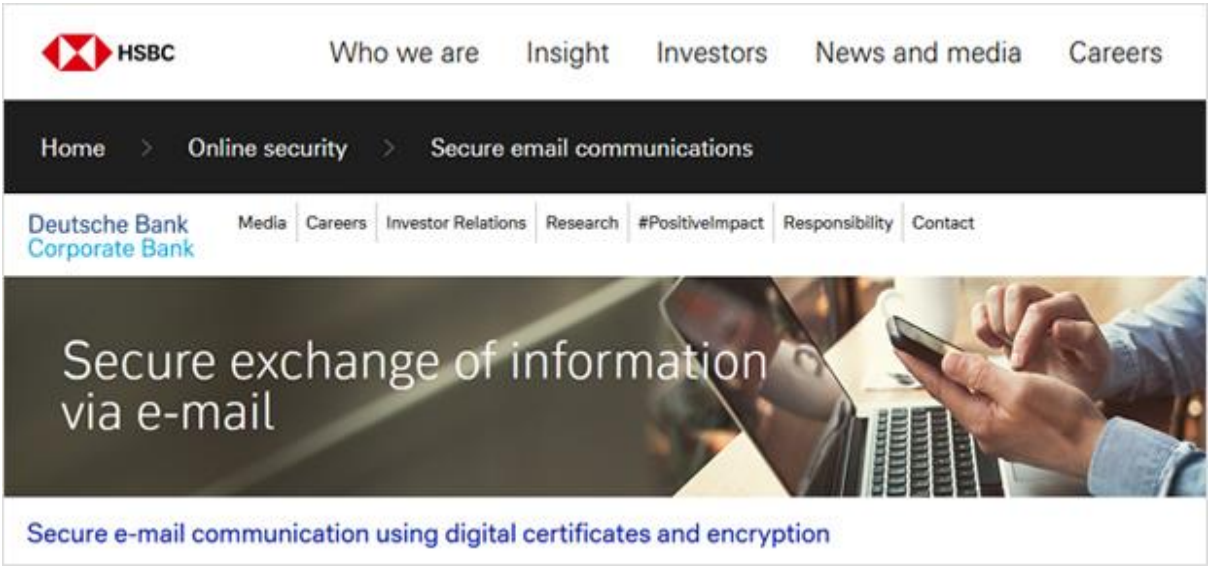
Is the "Secure email" sent by the Bank Really Secure?

(May 27, 2021)

The author checked the introduction of secure emails on the websites of more than 20 well-known banks around the world. The official websites of banks have introduced how the bank guarantees the security of emails sent to users, how to send encrypted emails to users, or tell users how to do and what to pay attention to.

The author believes that these are very good and necessary to tell bank users how to prevent fraudulent bank emails and how to use the encrypted email solutions adopted by the bank. Because bank emails contain a large amount of user financial confidential information, so the most fraudulent emails are financial fraud emails. Fraud emails induce users to click on the links to fake bank websites and require users to enter their bank cards and login passwords, so as to achieve the purpose of stealing users' bank accounts. Therefore, banks not only need to have a dedicated page to popularize email security knowledge, but also must adopt reliable technical means such as encrypted emails to prevent email fraud.



The author believes that the bank email security measures adopted by all banks still have some

shortcomings. This article is specially written to help banks recognize the shortcomings of their solutions and actively improve related technical solutions, continuously improve the security of bank emails to truly protect the security of bank users' accounts.

At present, in addition to telling users to pay attention to email security, most banks have also taken some technical measures to ensure email security. There are mainly the following three solutions:

(1) Adopt S/MIME digital signature and encryption technology.

This is the secure solution. The digital signature of the email can prove that the email is indeed from the bank, preventing fraudulent bank emails; while the email encryption can ensure the security of confidential information in bank emails and prevent illegal theft and illegal tampering of bank statement information. Deutsche Bank and Deutsche Post Bank adopted this solution.

The biggest problem with this solution is that it is very difficult to implement. It requires users to use email client software that supports S/MIME encryption, and users need to purchase and apply for email certificates from a trusted CA, and hardly to configure and use the email certificates. Only in this way can users decrypt the encrypted emails from the bank and can sent encrypted email to the bank. This solution has very high requirements on the user's IT level, which may affect popular applications.

(2) Adopt digital envelope and PGP encryption technology.

This is a compromise solution compared to the first and most secure solution, which reduces a certain degree of security and lowers the threshold for use. It is realized by webpage, the user only needs to register an account and set a password, log in to a special webpage to view encrypted emails from the bank and reply to the encrypted emails to the bank.

It can be seen that this solution is obviously much more convenient and simpler than the first solution. Users do not need to apply for a certificate from the CA, nor do they need to use a designated email client. Logging in to the web page can realize decryption and reading of encrypted email and send encrypted email to the bank. Some are for a PDF file encrypted with

a password, and some are for logging into a third-party encrypted email system to read and send encrypted email to the bank.

However, these schemes still send cleartext emails to users, notifying users to log in to the secure email system to view encrypted emails. For the first time, users must first use their own email address as a username to register for the secure email service provided by the bank. The cleartext notification emails, the registration process, and the process of entering a password are all insecure and may be attacked and the subsequent operations are insecure.

(3) Do not take any technical measures.

Send cleartext emails directly to users, such as credit card statements, and every consumption record is clear! This is the most insecure way. It can be said that this is the bank's negligence! This is the case with a certain bank I used. I had to ask the bank to cancel the billing email function. If it really can’t be cancelled, I had to modify it to a non-existent email address.

Some banks have improved a little bit, and only write a rough consumption statistic report, such as the total consumption of this month, the minimum repayment required and the required repayment date, etc., and the user needs to click the link to log in to the online banking system to view the detailed information. Some banks have adopted another method to abandon insecure cleartext emails and use online banking apps instead. This is of course safer than cleartext email, but the online banking app still has other security issues such as not using https encryption and not validating SSL certificates. Using email to achieve communication between the bank and the user is the best solution. It should not be discarded because of the security problem of the cleartext email. Instead, the email communication security problem should be solved.

Readers may ask, after talking about the so many bank email security issues, what should be done to make the most secure bank emails? It's very simple, the first solution is the most secure solution, because S/MIME encryption and digital signature are the best email security technologies. We only need to solve the problem of ease of use. After years of hard work, MeSign Technology has developed an automatic email client software that uses S/MIME technology - MeSign App and built a cloud cryptographic infrastructure. The "cloud" and

"client" work together, which completely solves the difficulty of S/MIME encryption and digital signature, bank users only need to set up their own email account in MeSign App, and then they can send encrypted emails to the bank and decrypt the encrypted emails sent by the bank. The banking business system also only needs to call MeSign public key API to retrieve the user's public key for free, then automatically send encrypted emails to the bank user.

More importantly, MeSign App provides a free edition, allowing users to experience the automatic email encryption service for free. Bank users are welcome to experience it for free, and interested banks are welcome to contact us at any time if they have any questions. MeSign Technology has provided an email encryption solution for Bangkok Bank, realizing that the email communication between the bank and bank users is encrypted and digitally signed, and MeSign Technology's global exclusive email time stamping service can satisfy the needs of banks and users for trusted time application requirements of the email communication.

---------- END ----------

Richard Wang

Digitally signed by Richard Wang
ceo@mesign.com

Want to contact me to discuss this topic? Please use MeSign App (-) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.