UniCredit Bank

Dear Client,

We would like to inform you about a type of fraudulent behaviour we, or our clients respectively, have come across during our work in the last few months. Fraudsters want to attain having funds sent from a corporate account, by hacking the corporate e-mail.

There have been some cases where the hacker penetrated ("hacked") the corporate e-mail completely unnoticed and started to track the relevant company's correspondence. From there, the hacker can track, for example, a communication with a supplier. Now, the hacker has information about what the company orders and how the supplier's invoices look like. At the right moment, the hacker sends a false invoice from the supplier's address. The victim of the hacking expects the invoice and is not vigilant. The invoice is completely identical, only with a different account number of the supplier. The victim of the hacking often asks "Do you really have a new account?", but if he/she sends the question by e-mail, the hacker will take care of it, intercepting the e-mail and confirming (in the supplier's name) that everything is all right.

A different form of the hack involves the hacker monitoring an e-mail of the company's senior officer (executive director/Board member/owner). The hacker tracks when such a person is outside the workplace and, afterwards, sends a brief e-mail from the address of such a person to a person authorised in the company to send funds. The order reads usually like this: "I need to have EUR xx.xxx sent to this account. It is really urgent, please inform me once you have done it". As a rule, such orders are mostly very urgent, they can be written in perfect language and they can be from an address of a person who is outside the workplace at that moment. Such orders involve sending funds abroad, often to a bank in the United Kingdom.

We recommend you contact the sender of the e-mail in person or by phone when you come across a suspicious case. In such situations, what is written does not necessarily have to be true.

A suspicious situation can be sending money to a new, unproven account.

If you suspect that you have been hacked, please inform your banker.

Yours faithfully,

Banking Security Unit
UniCredit Bank Czech Republic and Slovakia, a.s.