Moscow, August 30, 2016

CEO Fraud / Fake President Fraud / Business E-mail Compromise

Dear Business Partners,

"Fake President Fraud", "CEO Fraud" or "Business E-mail Compromise" is a social engineering attack in which a criminal tries to convince a member of the financial department of a company to send out a payment to the attacker's bank account. The attack can be divided into three steps:

- Establish Contact: Criminal impersonates a CEO, CFO or any other superior who has enough authority to arrange urgent payments. The attacker may use email accounts designed to approximate genuine corporate email accounts such as "michaelmiller@compaany.com" (often with extra vowels or other small misspellings)
- Request Payment Transaction: The attacker often uses email to contact his target. To succeed in this step, the criminal uses different elements to convince the target to be compliant to his request and send out the payment. In order to avoid that a target verifies the authenticity and validity of an order, attackers often label the request as "STRICTLY CONFIDENTIAL" or insert statements like "this project is still secret". The attacker creates a false sense of urgency in order to get the target to make a rushed judgment or a rash decision
- Transfer Money: If the attacker manages to convince the targeted employee to send out the payment, the money gets transferred to the bank account of the criminal

How to protect yourself?

Different organizational and technical steps can be performed to mitigate the risk of an incident:

- Email communication only should not be sufficient when authorizing large payments
- Develop and communicate guidelines and processes of how payment transactions need to be handled
- Employees should be aware of this kind of attacks
- Publish only necessary personal and financial information in social media and company websites
- Use a two-step (four–eyes) verification process when sending out large amounts of money to bank accounts
- Do not use personal email address for business purpose
- Always use email signatures / encryption when sending mails with confidential and / or sensitive content
- To avoid an e-mail from being hacked and used to perform a "CEO Fraud", a strong authentication method should be used in addition to a strong password policy

Moscow
ul. Bakhrushina 32/1
115054 Moscow, Russia
t +7 / 495 / 956 55 57
info@schneider-group.com

St. Petersburg
Business Center Petrovskiy Fort
Office 801-803, Finlyandskiy pr. 4a
194044 St. Petersburg, Russia
t +7 / 812 / 458 58 00
spb@schneider-group.com

Aktau
Business Center Grand Nur Plaza
Office 46, Microdistrict 29 A
130000 Aktau, Kazakhstan
t +7 / 7292 / 201 151
aktau@schneider-group.com

Almaty
Tole Bi Street 101, Block 9 B
050012 Almaty, Kazakhstan
t +7 / 727 / 355 44 48
almaty@schneider-group.com

Astana
Business Center "Saint-Petersburg",
Dostyk Ave. 20, 14th floor, office 1407
010000 Astana, Kazakhstan
t +7 / 7172 / 425 822
astana@schneider-group.com

Berlin
Ritterstrasse 2 B
10969 Berlin, Germany
t +49 / 30 / 615 08 918
berlin@schneider-group.com

Frankfurt
THE SQUAIRE at the Airport
Entrance 12, Office 616
60549 Frankfurt, Germany
t +49 / 69 / 959 32 51 78
frankfurt@schneider-group.com

Kyiv
Horizon Office Towers
vul. Shovkovychna 42-44
01601 Kyiv, Ukraine
t +380 / 44 / 490 55 28
kyiv@schneider-group.com

Minsk
ul. Surganova 29
220012 Minsk, Belarus
t +375 / 17 / 290 25 57
minsk@schneider-group.com

Warsaw
ORCO Tower, Office 17.02.
Al. Jerozolimskie 81
02-001 Warsaw, Poland
t +48 / 22 / 695 03 10
warsaw@schneider-group.com

What does SCHNEIDER GROUP do for its clients?

Many of our customers entrust their bank transactions / treasury function to SCHNEIDER GROUP. According to the four–eye principle two employees of SCHNEIDER GROUP are involved in the payment authorization process. Based on the headquarters decision, our Partner or Director can be assigned with the 1st signature right and can be included in the bank signature card. The 2nd level of the bank signature right is usually assigned to the senior accountant responsible for the project and the supervising Head of Accounting Group. Alternatively, the financial verification role is performed by an employee of the Internal Controls Department. All authorizations in the online banking system are done by both our employees only after getting approval from an appointed client's representative.

A Process Management Guide is implemented for each accounting project:

Responsible	Process steps
SCHNEIDER GROUP	The list of invoices sent for approval to authorized person
Client	Approval of payments provided by authorized person via email
SCHNEIDER GROUP	Currency control documentation and payments orders are prepared and uploaded to the online-banking system; email sent to the authorized person to release payments
Client	Authorized person signed payments and currency control documentation
SCHNEIDER GROUP	Bank statement upload and processing into accounting database, check of unreleased payments, informing the authorized person

We hope you find our newsletter useful. Should you have any questions or require our assistance with respect to the above, please contact our experts:

Alexander Koepcke
Director, Member of the Board
KoepckeA@schneider-group.com

Evgeny Polyanskiy
Security Manager
PolyanskiyEE@schneider-group.com

+7 / 495 / 956 55 57 | +49 (40) 226 33 760
www.schneider-group.com