Incident handling: A suspicious e-mail communication

Solution

This is a financial fraud aimed against our business partner. This is what happened in time sequence:

1. Somebody was pretending to be from Big Company by spoofing the e-mail headers and reached out to the business partner with a generic request of an unpaid invoice.
2. The IT Partner's mailbox was handled by Li Zhang, asking for updated bank info.
3. The fake Credit department sent the updated bank information. Notice that the attacker was trying to take money from the IT Partner, not from Big Company (!), which is unusual. The attacker was posing as a genuine employee with the name Irene Gonzales and using email address credit@bigccmpany.com (notice the incorrect c**C**mpany.com domain). You can see both the real email address and spoofed email address in the PDF file at the top email.
4. Li found this all strange and asked Peter to validate the request she received.
5. Peter requested Li to send those emails.
6. Li sent the PDF file with scanned emails they had with the attacker.
7. Peter forwarded the e-mail to the CSIRT (you and your colleague).

Debriefing

Asking Peter or Li for more information could delay the investigation for hours, maybe days, due to different time zones, vacations, or misunderstandings. After that, it might be too late, and the partner might send the money to the scammer.

Because of that, the users (Peter and Li) need a reply as soon as possible, as brief as "It's a fraud, don't send the money." The technical details and explanations are not necessary, as the regular users don't need to know them (and might not understand them). You need to react briefly, understandably, and provide precise instructions.

Also, remember to thank the user for his/her vigilance. As an incident handler, never communicate in a way that the user is annoying or stupid for not sending you more information. This way, the user might not contact you again next time, and fall victim to another scam.