



Links:

- <https://www.ic3.gov/media/2017/170504.aspx>
- <https://bec.ic3.gov/>
- Gilbert Chikli youtube video (AP interview):
- <https://www.youtube.com/watch?v=u3eCfcSdwal>

Special Agent Don Cavender
dlcavender@fbi.gov
703-686-6638

Special Agent Michael Miller
mbmiller@fbi.gov
703-686-6632

Prevention & Detection

- Use IC3 PSA section “Suggestions for Protection” for ideas for your security awareness training.

Response

Use IC3 PSA section “What To Do If You Are A Victim” to start building a response plan.

Within 48 hours:

- Report it to your bank, request the transfer be recalled
- Report it to your local FBI office ASAP and/or the FBI IC3 (ic3.gov) or bec.ic3.gov. The sooner it’s reported, the better the chances of recovering the funds.
- Preserve the emails (headers needed for incoming emails for account receiving the fraudulent instructions), possible intrusion vector? (phishing attempt(s)).
- Preserve the hardware that was possibly compromised
- Preserve the logs (email, remote access)

Washington Field Office

Criminal Division, Cyber Branch, CY-5
Criminal Intrusion Squad: Financially Motivated Cyber-Crime