THE CRIMINAL PLAYBOOK TRAINING

(18:18)

Employees at every organization must be aware of common, yet often sophisticated, tactics used by criminals. The criminal playbook often involves stealing money and/or data directly from an organization, convincing employees to send money directly (but unknowingly) to the criminal, or locking an organization's data for ransom. However, there are protective steps you and your organization can take today to avoid becoming the next victim of cybercriminals.

Briefly explain each example:

Four Key Levels in the Criminal Playbook
1. How a Criminal Takes Money Directly? System Level Fraud (0:56)
2. Efforts Used to Convince You to Send Money Social Engineering (1:10)
3. Can They Steal Your Data and Sell It? Cyber Theft (1:56)
4. Lock Up Your Data for Ransom Ransomware (2:23)

+1 678.466.2220
securetreasury.com
securitycourse@strategictreasurer.com

Please complete table below:

Type of Fraud	Protection Steps
Check Forgery (3:01)	• *Protect Account Numbers* •
ACH Fraud (3:32)	• • •
AP Vendor Master Record (4:08)	• •
Data Breach (4:54)	• • • •
Ransomware (6:33)	• • • •
Business Email Compromise (7:57)	• • • •
System Fraud (9:14)	• • • • • •

+1 678.466.2220
securetreasury.com
securitycourse@strategictreasurer.com

Please complete the following outline:

Five Action Steps to Prevent Data Theft (10:58)

1.

2. Reconciliation
- Rapid
- Four Types
  - *Bank Reconciliation*
  - *Treasury Proof*
  -
  -

3.

4.

5.

Additional Notes

+1 678.466.2220
securetreasury.com
securitycourse@strategictreasurer.com