Scam alert on

APTs (Advanced Persistent Threats)

How the scams work

1. Clever hackers, typically backed by secretive government agencies, terrorist groups or criminal gangs, set their sights on a specific organization (such as a bank), researching the target in detail to find its weak points.
2. When they are ready, they attack the organization's IT networks and systems, infecting them with sophisticated custom-made spyware.
3. The spyware 'digs in', successfully hiding from antivirus and other security tools.
4. The hackers remotely-control their spyware through the Internet, snooping around the IT systems and networks, learning about the target then compromising and exploiting valuable information – especially financial information.
5. So long as it remains undetected, the attack continues for months, maybe *years*.

Avoid the scam

- You are our first line of defense! We are depending on business people to help us spot and resist APT attacks.
- Be *very* suspicious of links in emails. Hover the cursor over a link to check the address and only click it if you are sure it is safe.
- Avoid dubious websites, online ads, apps and unofficial app stores like the plague!
- Be *extremely* suspicious of email attachments and downloads from the Internet.
- Don't just ignore things that strike you as a bit *odd* – office visitors you don't recognize, missing files, strange phone calls, unexpected business failures, discrepancies in bank/credit card statements and so forth. Your gut instinct may be right on the button!
- Report your suspicions to your manager or call the Help Desk. It may just turn out to be an APT incident that nobody else has spotted, in which case you are in for a substantial reward!

More information

Browse the intranet *Security Zone* or contact the Help Desk for more on APTs, spyware, ransomware, antivirus, scareware, online banking Trojans, viruses, worms and other malicious software (malware).