Insider Threats: 3 Types of Users

Barracuda
Your journey, secured.

Careless Users

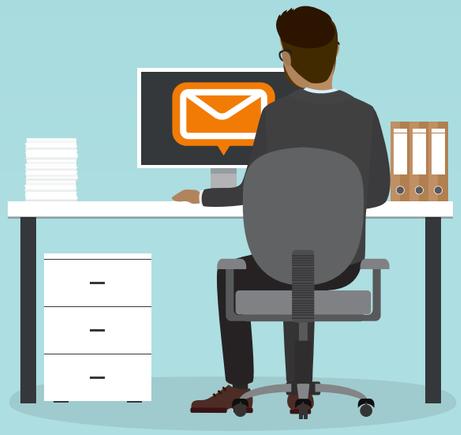
- Bypass security procedures for reasons of convenience or lazyness
- Believe protocols are a hassle or a waste of time

Examples

- Fail to lock devices when not at their desk
- Leave written passwords at desk

How to Deal with Threat

- Training that emphasizes the harm they could inflict
- Let them know the penalties they could suffer, if their habits don't change



Compromised Users

- Victims of spear phishing attacks or social engineering.
- Don't realize it until it's too late

Examples

- Employee who clicks a link in a phishing email that triggers a ransomware attack
- Accounts payable associate who's tricked into wiring money to a fake account
- Anybody can be a target for scammers
- Make up majority of inside threats

How to Deal with Threat

- Technologies such as firewalls and anti-phishing software that can flag harmful emails
- Training that helps employees detect phishing and social engineering can help

Malicious Users

- May be motivated by greed, a desire for revenge, ideology, or any number of other reasons
- Highly motivated and can cover their tracks
- Can do significant harm over extended time period

Examples

- Foreign national who takes a contracting position and sends sensitive data back to homeland operatives
- IT manager who sells customer account information to criminals

Warning Signs

- Large data transfers
- Unexpected or incorrect access requests
- Multiple failed logins
- Service account abuse
- New activity on dormant accounts
- Off-hour network traffic
- Interactions with users or locations you don't normally deal with