Intrada
TECHNOLOGIES

Understanding Phishing Scams

Phishing attempts don many masks, from deceptive emails masquerading as messages from reputable brands to counterfeit websites designed with the sole intent of harvesting personal information. Below, we delineate essential insights and common strategies utilized by cyber adversaries aiming to breach your data security. Intrada Technologies is dedicated to safeguarding your digital infrastructure against such threats, providing the expertise and solutions needed to combat phishing attempts effectively.

Intrada Technologies suggest every email get applied these two basic filters:

1. **Was I expecting it?** If not, take extra time to review and confirm the source and context before clicking on any links. Don't jump to conclusions or get rushed. If it was really important, it should not be an email.

2. **Always verify any account, financial, or personal record modifications by cross-checking with the "sender" through an alternative communication channel.** The crucial step is to validate using a different method of contact. For instance, if you get an email, make a call to confirm. If you receive a phone call, send an email for any further correspondence.

The most used techniques in phishing scams are often those that play on human psychology:

1. **Urgency**: Prompting quick, emotional reactions.
2. **Authority**: Emails claim to come from a credible source, like a CEO or institution.
3. **Familiarity**: Scammers may pretend to be friends or colleagues to gain trust.
4. **Rewards**: Offering "too good to be true" prizes to entice victims.

31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding
Expectations.