Cyber Security Awareness Training

Social Engineering Vishing

Hacking is viewed as highly technical. But it makes sense to try to exploit people before spending time and effort on more complicated methods.

Vishing is an attack performed by phone (voice) rather than by email. This involves impersonating a colleague (e.g. IT Department) or friend, for example, on a social networking site to obtain additional personal information, possibly in preparation for a larger attack (see: spear phishing).

Why Does it Work?

- If we haven't been directly burned before, we're not suspicious.
- Don't want to seem paranoid.
- Don't want to be uncooperative.
- Most people don't want to refuse a request.
- It's nice to be nice.
- Say yes, it's done and out of the way.
- Say no, you must explain.

Indicators

- Refusal to leave a phone contact.
- Quickly on and quickly off the line.
- Chattiness, though you've never met.
- Quickly brings up office gossip to establish trust & insider status.
- Meandering conversation leading to an urgent request.

Subtle Signs

- Failure to use standard corporate buzzwords and jargon.
- Sounds like an outsider.
- Doesn't know how things really get done here.
- Sounds unnatural, stilted.
- Incorrect phrasing of standard things.
- Heavy referencing of higher-ups as drivers of the request for information.

Do trust your judgment: if it sounds fishy, it probably is!

Source: www.ftc.gov
Powered by Sonic Performance Support
Hamburg, Germany