FORGE

The Arkansas Cyber Defense Center

Business Email Compromise

Business email compromise (also known as email account compromise) is a social engineering attack in which an adversary sends an email that appears to be from a legitimate source such as a vendor, management official or a third party contractor making an illegitimate request.

Techniques:

Social Engineering: Adversary uses psychological deception to manipulate users into giving away sensitive information

Spoofing: Cyber criminals masquerade as a trusted individual or organization.

Public-Facing Application Exploitation: May attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.

Who could be targeted?

High-level management personnel such as board members and accounts payable personnel are favorite targets.

Why be aware of this attack?

Attacks of this type can lead to significant financial losses, loss of trust between third party vendors, and operational disruptions from lost access to email.

What do threat actors want?

Adversaries seek sensitive information and financial exploitation.

Prevention tips:

- Focus on personal training in the office and on home networks.
- Set up secondary checks outside of email to confirm purchase orders.
- Be wary of impatient requests. Urgency is often used to circumvent security checks.

POWERED BY SBA U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599