Accounting and Finance Employees – Beware of A/R phishing fraud

Danger

Cybercriminals are targeting accounting and finance employees in a new scam involving accounts receivable aging reports. The cybercriminal will impersonate a high-level person at an organization and ask for a copy of the report and payment contacts.

The cybercriminal then contacts customers with outstanding invoices, posing as a credit and collections employee. The criminal may offer discounted payment terms as an incentive and will supply new payment instructions for an account controlled by the cybercriminal. If the customer falls for it, the cybercriminal gets paid and we don't.

How to spot an A/R phishing e-mail

- The sender claims to be traveling and available only by email

- The sender claims to need the information urgently

- The request is formatted to look like it's sent from a mobile device in order to make it harder for you to recognize that something is off

- The sender's email address will be similar to our CEO/CFO's – often off by only a character or two. For example,

    CEO@company_xyz.com versus
    CEO@company-xyz.com

- The initial request may be for the aging report, and a request for payment contacts may follow.

Tips to protect yourself

- Get verbal confirmation from the person supposedly making the request

- Know our procedures for handling legitimate requests for this type of information

- Carefully confirm the email address that the message was sent from

- Report any phishing attempts immediately.

Who?
The request is usually made to look like it comes from the CEO, CFO, or other high level executive.

How?
The request typically comes by email.

What?
Requests may look like this:

> I need you to email me the aging report from A/R, and also include customer payable contact email on this report.

When?
May occur at any time, but particularly at end of year and end of quarter.

And that's not all

This is one form of a scam known as CEO fraud. A similar but unrelated scheme is for the cybercriminal to request a PDF copy of employee W-2s, which can be used to file fraudulent tax returns.