Email Scams

An email attack isn't particularly difficult to pull off and can be quite lucrative for cyber criminals. A common form of email attacks is called a Business Email Compromise (BEC). In its basic form, a BEC is when an attacker impersonates an authority within an organization and convinces someone else in that organization to perform an action, such as a wire transfer or to provide W-2 information. It is simple, but also incredibly effective.

Information on a W-2 document is particularly valuable. In fact, as part of what the Darknet world calls a “fullz” that information can be worth $25-30 per record. A “fullz” includes a collection of information such as name, social security number, date of birth, account numbers, etc. If someone obtains hundreds or thousands of W-2s it can fetch quite a payoff.

Create the Culture

Having processes in place to avoid having this happen at your organization is crucial. Employees should not have access to all of the sensitive data in a record without some sort of oversight. It's important to put controls in place so that if anyone asks for such information, it's discussed and approved by multiple people. One of the questions that should be asked is “why does this person need this information?” Then it should be verified with the requester via voice or some other way that does not include replying to an email request. While email and text are acceptable ways to communicate in most instances, voice interaction goes a long way to prevent scams such as these from being a huge success.

Employees might feel a bit insecure about asking someone who claims to be the CEO why he or she needs personal information, but if it's legitimate that executive will appreciate the fact that you checked before giving it up.

Get the lastest information from our website. Scan the QR Code to go directly to this page.