What is an impersonation attack?

An impersonation attack is a form of fraud in which attackers pose as a known or trusted person to dupe an employee into transferring money to a fraudulent account, sharing sensitive information (such as intellectual property, financial data or payroll information), or revealing login credentials that attackers can used to hack into a company's computer network. CEO fraud, business email compromise and whaling are specific forms of impersonation attacks where malicious individuals pose as high-level executives within a company.

How does an impersonation attack work?

Impersonation attacks are typically malware-less attacks conducted through email using social engineering to gain the trust of a targeted employee. Attackers may research a victim online, gathering information from social media accounts and other online sources which, when used in the text of an email, can lend authenticity to the message. An impersonation attack is typically directed at an employee who can initiate wire transfers or who has access to sensitive or proprietary data. The employee receives an email that appears to be from a legitimate source, often a high-level executive within the company, urgently requesting that money be wired to a certain account or that sensitive information be sent immediately.

How to recognize an impersonation attack?

Unlike common phishing attacks, which are often unspecific and filled with grammar or spelling mistakes, impersonation attacks are highly targeted and well-crafted to appear realistic and authentic. There are a few things, however, that point to a potentially fraudulent email:

- An urgent and possibly threatening tone. Most impersonation attacks request or demand that the recipient act immediately. Some impersonation emails may threaten negative consequences if the recipient doesn't act quickly enough. This is intended to prevent the employee from taking time to double check before acting.
- An emphasis on confidentiality. Some impersonation attacks will suggest that the action is part of a confidential development or secret program that should not be discussed with colleagues or immediate superiors.
- A request to send money or share sensitive information. Any request to transfer money or to release sensitive financial data, payroll information or intellectual property should be corroborated through multiple channels.
- A problem with email addresses or links. Often, the email impersonating an executive will be a slightly altered version of a legitimate email address. Additionally, the reply-to address may be different than the sender's address, or the actual links to URLs within the email don't match the text in the hyperlinks in the body of the email copy.
- Unusual requests or accounts. Impersonation attacks frequently request recipients to send money to bank accounts or vendor accounts that have different numbers than the employee has used in the past.