Scamming

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

With email scamming, cybercriminals use fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information. Examples include fake job postings, investment opportunities, inheritance notifications, lottery prizes, and fund transfers.

Scammers prey on an individual's sympathy, charity, or fear. Unfortunately, many individuals fall for email scams, unwittingly sharing sensitive information or making payments to scammers.

Scam phishing emails can be recognized by their clues:

• A sender address you don't recognize or doesn't make sense.

• An empty 'To' address field or one that's filled with names you

 don't recognize.

• A send date or time that falls outside normal business hours.

• A heightened sense of urgency or alarm.

• Promises of rewards or threats if you do or don't act.

The sample email highlights some of the clues you can watch for.

Example

Greetings {email.fullName},

My name is Mike Johnson and I am an investment broker. I want to inform you that I represent an Investment Group called PillarTree Investments. We are expanding our global presence by investing in viable projects across the globe, as well as assisting businesses to grow in this trying time of the covid 19 pandemic. We are willing to inject $1 million to $300 million or more in a viable project.

We grant our funding at a 4% ROI per annum for 10 years and 12 months moratorium. If you have a viable project that needs funding, kindly get back to us with your business plan and executive summary for our review and possible funding.

Regards,

Mike Johnson

Mike Johnson
Client Executive/Broker

An email that arrives unsolicited offering financial rewards is always some form of scam.

Don't be fooled by highly technical or sophisticated content that's designed to entice you to act.

The highly designed logo, header and 'personalized' sign-off look convincing, but a web search of the company and sender would reveal they don't exist.

Email Protection