proofpoint

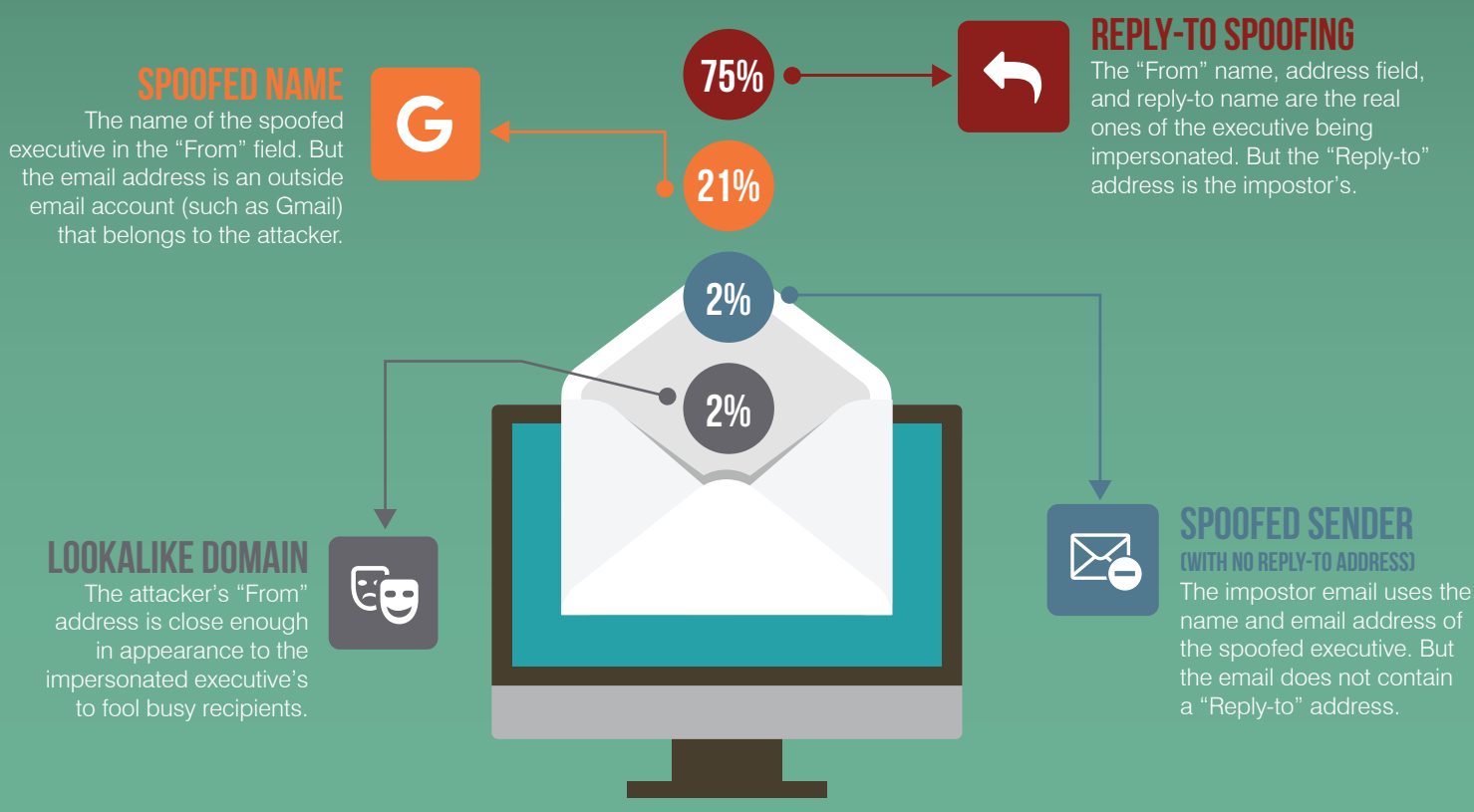
IMPOSTOR EMAIL THREATS

What You Need to Know to Recognize and Stop Them

Impostor email threats (also called business email compromise and CEO fraud) have hit more than 17,000 companies since the FBI's Internet Crime Complaint Center (IC3) began tracking this type of scam in late 2013. These attacks have collectively scammed victims out of more than $2.3 billion globally. Many messages will be quickly recognized by recipients as phishing and discarded. But the small few that succeed can yield millions of dollars in fraudulent transfers.

Here are some facts about impostor emails from Proofpoint research.

4 TYPES OF IMPOSTOR EMAILS



SPOOFED NAME

The name of the spoofed executive in the "From" field. But the email address is an outside email account (such as Gmail) that belongs to the attacker.

REPLY-TO SPOOFING

The "From" name, address field, and reply-to name are the real ones of the executive being impersonated. But the "Reply-to" address is the impostor's.

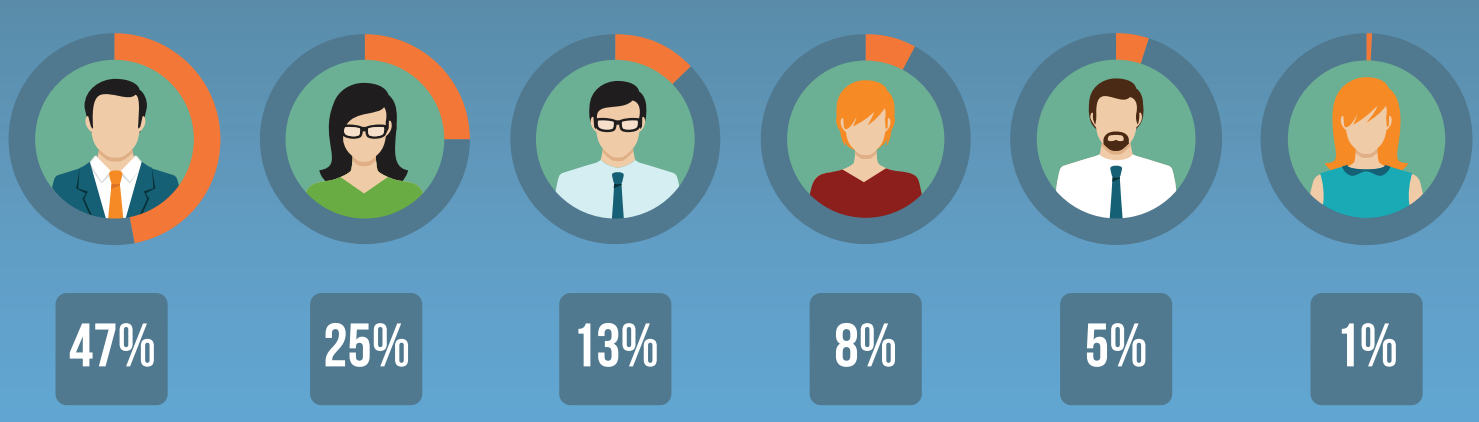
LOOKALIKE DOMAIN

The attacker's "From" address is close enough in appearance to the impersonated executive's to fool busy recipients.

SPOOFED SENDER (WITH NO REPLY-TO ADDRESS)

The impostor email uses the name and email address of the spoofed executive. But the email does not contain a "Reply-to" address.

IMPOSTOR EMAIL TARGETS



IMPOSTOR EMAIL TOPICS

TO LEARN MORE ABOUT THE THREAT OF IMPOSTOR EMAILS VISIT WWW.PROOFPOINT.COM