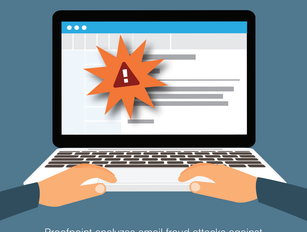
proofpoint.

PROTECTING YOUR PEOPLE
Q3 2017 EMAIL FRAUD THREAT REPORT

Email fraud is one of today's largest cyber threats. Unlike other cyber threats, email fraud exploits people rather than technology. By preying on human nature, attackers steal money and valuable information from employees, customers, and partners.



Proofpoint analyzes email fraud attacks against thousands of organizations around the globe.
Here are our findings for Q3 2017.

ORGANIZATIONS ARE UNDER ATTACK MORE THAN EVER

12% increase in targeted attempts per organization (vs. previous quarter)

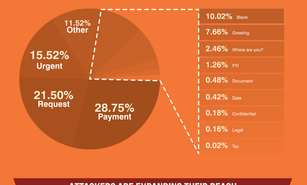
49% of all companies were targeted with more than 10 email fraud messages

ATTACKERS ARE GROWING MORE SOPHISTICATED

Attackers are finding new ways to deceive security technology and the people who rely on it.
The change suggests that attackers are trying to appeal a range of personality types.

Subject lines that included "request" rose **43%** over the previous quarter

Subject lines with "urgent" fell by **21%** in the same period



ATTACKERS ARE EXPANDING THEIR REACH WITHIN TARGETED ORGANIZATIONS

73% of organizations had multiple identities spoofed and more than one employee targeted

28% more people targeted per organization on average

DOMAIN SPOOFING ATTACKS EXPAND THEIR FOOTPRINT

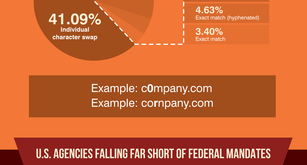
5% increase in domain spoofing attacks

89% of organizations were targeted by at least one domain spoofing email

LOOKALIKE DOMAINS ALSO A PROBLEM

Lookalike domains—in which attackers register a domain that's confusingly similar to the real one—is another leading spoofing technique.

Here are the most common approaches to creating lookalike domains.

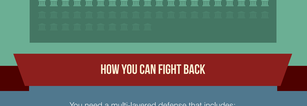


Example: c0mpany.com
Example: cornpany.com

U.S. AGENCIES FALLING FAR SHORT OF FEDERAL MANDATES

1 in every 8
emails sent from a federal agency is fraudulent

100 of the 133
federal agencies identified by Binding Operational Directive 18-01 have no published DMARC policies.



HOW YOU CAN FIGHT BACK

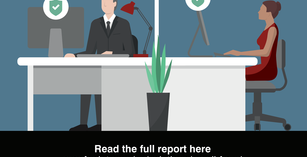
You need a multi-layered defense that includes:

DMARC email authentication.
Block all impostor email attacks that spoof trusted domains.

Dynamic classification.
Analyze the content and context of the email and stop display-name and lookalike domain spoofing at the email gateway.

Data loss prevention.
Prevents sensitive information, such as W2s, from leaving your environment.

Lookalike domain discovery.
Identify and flag potential risky domains outside of your control.



Read the full report here
proofpoint.com/us/solutions/email-fraud