proofpoint.

EMAIL FRAUD: 3 TARGETS, 3 TACTICS, 3 REASONS TO CHOOSE PROOFPOINT

Email fraud is costing organizations of all sizes and in all industries billions of dollars. These highly targeted email spoofing attacks are socially engineered to target people rather than technology. Email fraud is a 360-degree problem that puts several stakeholders at risk and includes multiple identity deception tactics.

3 Targets

Attackers can target multiple stakeholders related to your business:

1. **Your employees**—Business email compromise
2. **Your customers**—Consumer phishing
3. **Your partners**—Supply chain spoofing

Email fraud has cost organizations more than **$12.5 billion** since the FBI began tracking it in late 2013. The average attack nets about $159,000 USD.

Source: FBI

3 Tactics

Fraudsters leverage multiple identity deception tactics to avoid being blocked:

1. **Display name spoofing**—The display name is what appears in the “From:” field when reading the email. It’s the easiest email identifier to manipulate.
2. **Domain spoofing**—An exact match of the organization’s domain is used to launch this type of email fraud attack.
3. **Lookalike domains**—Third parties can register lookalike domains and send email that look like it’s coming from a trusted source.

TACTIC EXAMPLES

Display name spoofing
<John Smith>

Domain spoofing
yourcompany.com

Lookalike domain
y0urc0rnpany.com

3 Reasons to Choose Proofpoint

Proofpoint EFD360 protects your employees, customers and partners from every form of email fraud. It provides:

1. **360-degree protection**—The security controls you need to block email fraud attacks before they reach the inbox.
2. **Greatest efficacy**—Extensive, proprietary data sources ensure accuracy and reduce risk.
3. **Proven implementation**—Full visibility across all targets from a single console and a staff of DMARC authentication experts help you every step of the way.

There are **5-10 billion** emails processed daily across **7000+ enterprise customers**, **40,000+ SMBs**, **120+ ISPs** and more.

SECURITY CONTROLS

Email authentication (DMARC)
Prevents domain spoofing and ensures that email comes from who it says its coming from.

Machine learning and policy
Identifies and blocks fraudulent emails—including display name spoofing and lookalike domains—that target your organization.

Domain monitoring
Detects and analyzes potentially risky lookalike domains registered by third parties. It also surfaces all your brand-owned domains that can be protected from impersonation.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today’s mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint. proofpoint.com