Domain Spoofing: A Widespread Risk at PE Firms & Portfolio Companies

In short:

55 percent of mid-market PE firms and portfolio companies are vulnerable to domain spoofing, which enables phishing. No firm is fully protected across its portfolio. We've ranked the top 20 firms based on their level of protection.

1. Executive Summary

Spoofing, where attackers send phishing emails from addresses that appear to be legitimate, is a major contributor to cybercrime. Organizations can protect their own domains from being spoofed, but many do not. Our analysis of 159 middle-market private equity (PE) firms and their portfolio companies determined that most domains are insufficiently protected from spoofing, and that 21 percent are fully vulnerable. No PE firm is completely protected across its full portfolio.

This gap in protection is unsurprising, because penetration tests, vulnerability scans, and security audits often overlook domain spoofing risks. Additionally, implementing the necessary security measures (SPF, DKIM, and DMARC) can be tricky, leading many companies to only partially resolve the problem.

This research brief explores the nature of the threat and why it is especially serious for PE firms and portfolio companies, ranks PE firms based on how well they are protected, and provides clear solutions to stop domain spoofing.

2. The Spoofing Threat

Cybercriminals spoof domains to trick email recipients into thinking a message is legitimate. Spoofing is a primary enabler of phishing attacks, which lead to breaches and financial losses.

The risk is especially severe for private equity firms and their portfolio companies. These high-value targets hold sensitive financial data, and operate in a complex, interconnected system with frequent, high-stakes communication. Phishing emails that appear to come from a trusted partner or executive in these environments are likely to be acted on quickly, especially when they create a sense of urgency or financial importance.

Phishing often enables man-in-the-middle attacks, allowing cybercriminals to tamper with financial data and direct funds to offshore accounts. By the time the victim becomes aware, it's too late.

3. Preventing Domain Spoofing

Many organizations focus on training employees to recognize phishing attempts, but they often overlook a more fundamental vulnerability: their own improperly configured domain settings.

Domain spoofing can be prevented by configuring email authentication protocols correctly. Three key technologies—SPF, DKIM, and DMARC —work together to ensure that only authorized senders can use a domain.

When implemented well, these protocols provide a robust defense against domain spoofing. However, many organizations either fail to implement them correctly or neglect them altogether, leaving their domains exposed.

4. Research Insights: Domain Spoofing Vulnerabilities in Private Equity

Atumcell conducted an in-depth analysis of 159 middle-market private equity firms and their 2734 current portfolio companies, evaluating their use of SPF, DKIM, and DMARC. The results reveal that most domains are spoofable:

- **21 percent** of domains are fully vulnerable to spoofing.
- **An additional 34 percent** of domains are partially protected. Emails can be spoofed, but will be recognized as fake and rejected by some, but not all email clients.
- **45 percent** of domains are fully protected, which is encouraging and demonstrates that mainstream organizations can configure their domains properly.

Results are somewhat better when analyzing the PE firms themselves, while excluding portfolio companies:

- **15 percent** are fully spoofable.
- **26 percent** are partially protected.
- **59 percent** are fully protected.

These findings actually understate the risks. That's because only the company's primary domain is included in the analysis. Many companies have additional URLs that are familiar to customers (for example Atumcell has Atumscan.com in addition to Atumcell.com). Such domains can be spoofed, even if the legitimate owner does not use them to send email.

5. The Rankings

To generate the rankings, we assigned a risk score to each domain. Fully protected domains were scored as 0, partially protected domains as 50, and fully spoofable domains as 100. We averaged the results for the PE firm and its portfolio companies to generate a composite score, where 0 means all domains are properly protected and 100 means none are protected. Visit atumcell.com/spoofmethod for the detailed methodology.

No PE firm and portfolio were perfect, but some did quite well. The top 20 performers are as follows. Lower scores are better.

Top 20 PE Firms in Managing Spoofing Risk

Rank	PE Firm	HQ	Score
1	Pritzker Private Capital	Chicago	8.3
2	Crosspoint Capital Partners	Menlo Park	10.7
3	Tailwater Capital	Dallas	13.6
4	FTV Capital	San Francisco	14.0
5	Baird Capital	Chicago	14.6
6	Align Capital Partners	Dallas	15.9
7	Pamlico Capital	Charlotte	18.0
8	Serent Capital	San Francisco	18.1
9	Lightyear Capital	New York	18.4
10	Sageview Capital	Palo Alto	19.6
11	Morgan Stanley Expansion Capital	New York	19.8
12	DW Healthcare Partners	Park City	20.0
13	Bregal Sagemount	New York	20.3
14	Graham Partners	Newton Square	20.5
15	BV Investment Partners	Boston	21.7
16	Madison Industries	Chicago	22.4
17	River Associates	Chattanooga	22.7
18	OceanSound Partners	New York	22.7
19	Further Global	New York	23.1
20	Riverside Partners	Boston	23.1

6. Protect Your Firm and Portfolio Companies

Private equity leaders should engage with their technical teams to review domain configurations for SPF, DKIM, and DMARC. Atumcell offers a technical guide that lays out the steps.

Extend spoofing protection to other domains associated with your brand, even ones that do not have email set up. A user could still be tricked into clicking a link from a domain that doesn't normally send email, as long as it's familiar.

Visit atumcell.com/spoofcheck to determine whether any site you're visiting is spoofable. This is a good way for non-technical managers to validate that settings have been properly configured.

7. Atumcell's Role in Enhancing Cybersecurity for Private Equity

Atumcell provides a cybersecurity operating system for private equity, empowering PE firms to monitor, manage, and report security vulnerabilities at the portfolio level, and track portfolio company progress. Our advanced penetration testing offers comprehensive validation of your security measures.

Contact info@atumcell.com or call David Williams at (617) 671-8810 to discuss.