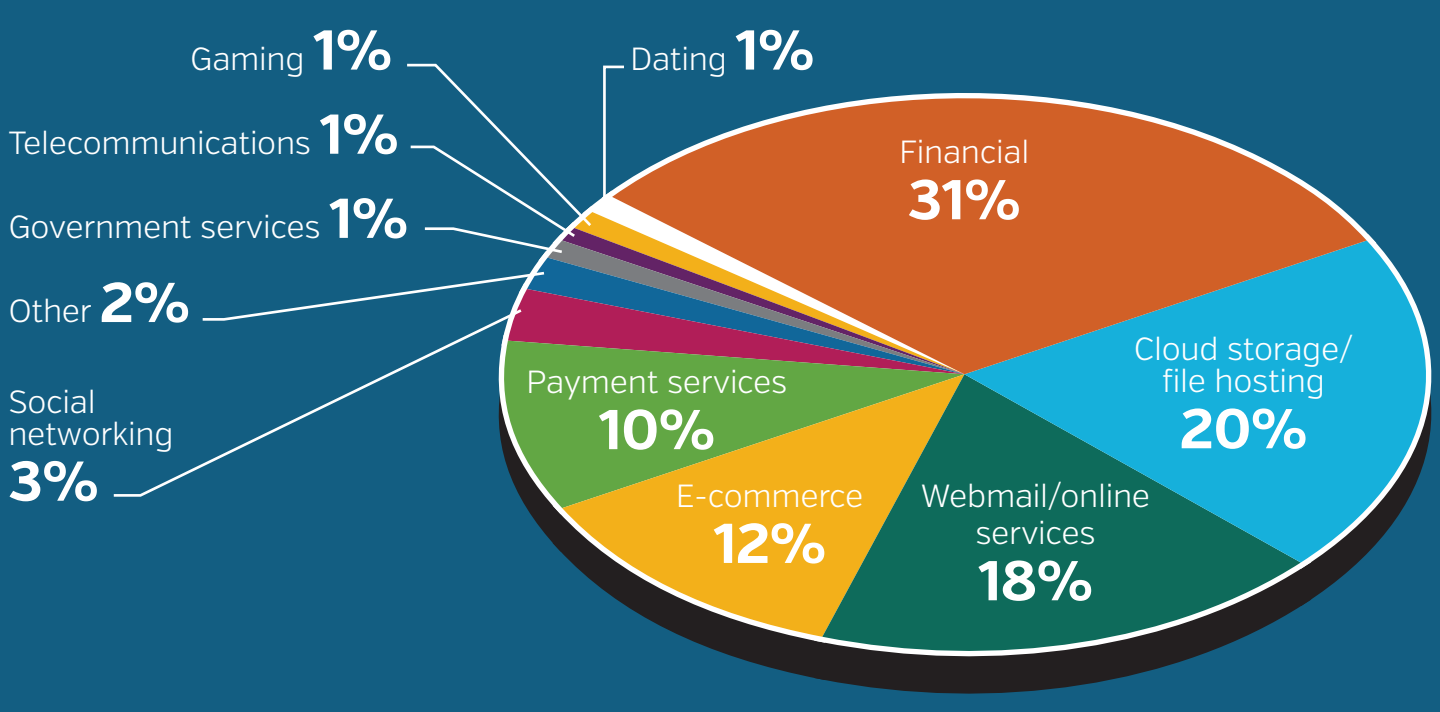
When the boss gives you an order, it might not be the boss

Spear phishers select specific targets, mine company websites for ways to steal

More spear phishing attacks are targeting the assets of a specific organization through emails purportedly sent to staff from their CEOs, according to a study by PhishLabs. Such attacks aren't scattershot, but narrowly distributed and customized to each target. The number of organizations targeted with Business Email Compromise spear phishing attacks grew tremendously in 2015.

They go where the money is

The most targeted industry in 2015 was financial institutions, followed by cloud storage/file hosting sites, webmail/online services, ecommerce sites, and payment services. Companies in these five industries made up more than 90 percent of all phishing targets in 2015. Cloud storage/file hosting services accounted for nearly 20 percent of phishing attacks, a 157 percent increase.



It's less and less likely to be random

Business Email Compromise attacks are increasing, making it appear as if employee email accounts are compromised. They're a form of wire fraud, similar to fake invoicing scams, also known as executive impersonation scams and CEO fraud. A majority (77 percent) of companies targeted by phishing attacks in 2015 were in the United States. Far behind were China (5%), France (3%), Great Britain (3%) and Australia (2%).

Increasing

United States

2015	76.8%
2014	71.2%
2013	70.4%

China

2015	5.4%
2014	4.1%
2013	1.1%

Decreasing

Great Britain

2013	7.5%
2014	6.2%
2015	3.0%

Germany

2013	5.5%
2014	1.9%
2015	1.5%

Companies can make it easy for bad guys

In many cases, targeting requires little effort, with attackers getting information from public sources and business-networking sites. Companies often: post full names, titles and email addresses for executive team members on their websites; post personal names, email addresses and direct numbers in accounting/billing contact information; and use consistent systems for email addresses. More than half of phishing sites were registered with the .com top-level domain.

More than one way to scam a business

There are several types of BEC attacks. The traditional version uses an email sent to a staffer that appears to be from the company's CEO. A newer type uses a mergers-and-acquisition strategy that reinforces the need for secrecy and includes quotes from lawyers.

Source: PhishLabs 2016 Phishing Trends & Intelligence Report: Hacking the Human