Spoofers Target CFI Customers

cyber security employees

Summary: A June 2022 report from Allure Security, a cybersecurity firm that specializes in protecting financial institutions, says that about 20% of CFI's are the targets of website impersonation attacks. Rather than simply assume that website impersonation attacks are something that happens to larger banks, CFIs should be proactive about protecting themselves and their customers from this kind of fraud. We explore a few tactics to keep your CFI and your customers safe.

When the film "Catfish" debuted in 2010, most viewers weren't familiar with "catfishing" — using a fake online identity to target another person for personal financial gain or other exploitative goals — and many more thought the plot unlikely. How could a young man be so easily fooled into thinking the woman he was talking to was real, despite all the red flags that she wasn't? Eight seasons and 205 episodes into a TV show based on the premise of helping victims catch their catfish, it seems this phenomenon is not so uncommon after all. Similarly, most people believe they would never walk right into a cybercriminal's trap, but the prevalence of cybercrime proves otherwise. Regular citizens are more vulnerable than they think.

Spoofers, also known as website impersonators or phishers, are cyber criminals who send urgent text messages or emails masquerading as a legitimate company. Their purpose is to steal the recipient's information or get them to download malware that harms their devices. The spoofers' messages are usually regarding refunds, accounts being suspended, overdue bills, or even money-saving offers designed to lure their target in by clicking the provided fake link.

The link will look like it goes to a legitimate website — but it's ever so slightly different than a genuine link would be. It might include a zero instead of the letter "o ," for instance, or add a number to the company name, like www.amaz0n.com instead of amazon.com. URL shorteners, like bit.ly, can also be used by spoofers to mask the real link address, taking a hacker site's URL and making it short and void of identity. It's easy for a victim who doesn't read very carefully to be fooled into visiting the scam web site and handing over account logins, private information, or credit card numbers.

Who do spoofers impersonate?

The most-spoofed company is LinkedIn. More than half of worldwide phishing attacks feature a fake LinkedIn landing page, while 14% of attacks happen to DHL. Google, Microsoft, WhatsApp, Amazon, Maersk, AliExpress, and Apple round out the top 10 most-spoofed companies.

In the financial world, spoofers often pretend to be big banking institutions, such as Chase or Bank of America. A recent report by Allure Security, however, says that customers at community financial institutions (CFIs) are spoofing victims, too.

CFI customers are targets, too.

The study, which looked at a random sample of banks and credit unions with less than $150B in assets during Q1 of 2022, showed that spoofers also impersonate roughly 20% of smaller financial institutions. The study

detected spoofing attacks against 164 of the 864 CFIs it monitored. The average institution experienced five attacks during the three-month study, while one brand experienced a shocking 154 attacks, for an average of 1.7 attacks per day.

"*This volume of attacks proves that scammers have regional banks and credit unions in their crosshairs," the Allure Security report says. "These institutions can't afford to consider themselves undeserving of scammers' attention.*"

How can CFIs protect themselves and their customers?

Both technology and customer education offer ways to guard against spoofing attacks. Methods include:

- **Multi-factor authentication.** When customers who are used to multiple requests for authentication on their CFI's site notice these measures missing, that can signal to users that something is wrong. Multi-factor authentication can also help keep customer data safe on the CFI's end, which prevents spoofers from harvesting your customers' contact information.
- **Software updates.** Increasing security measures and upgrading to new software that has protections against the most common cyber threats can also help keep customer data out of thieves' hands.
- **Customer education.** Communicate to customers what kind of communications to expect from you and what requests you will never make. Show them examples of how cleverly spoofers can disguise their real intentions. Finally, remind customers how to contact you if they have any questions about the legitimacy of an email or text message they've received.

The risks are only increasing for your customers to become targets. With security updates and a dedication to cyber safety education for your customers, you can keep your CFI safe from cyber risks.

ATTRACT NEW CUSTOMERS WITH INTERNATIONAL SERVICES

Help new customers with their cross-border commerce using seamless international services from PCBB. It is like having your own international department on call. Learn more today.

ECONOMY & RATES

Rates As Of: 09/08/2022 08:23AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	3.07	0.11	3.01
6M	3.42	0.10	3.23
1Y	3.60	0.09	3.21
2Y	3.50	0.00	2.76
5Y	3.40	0.05	2.14
10Y	3.29	0.10	1.78
30Y	3.44	0.15	1.54
FF Market	**FF Disc**		**IORB**
2.33	2.50		2.40
SOFR	**Prime**		**OBFR**
2.28	5.50		2.32