CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

# *Meeting the Challenges of Attacks, Breaches & Compliance*

First and foremost, credit unions must accept that they are being actively targeted by cybercriminals. The question is no longer “if” a credit union will be attacked but “when” and how to respond. Ultimately, if your members can get to their accounts online, so can cybercriminals. These best practices will help mitigate exposure to risk:

- Constantly educate your members – even incremental improvements to the “human firewall” of your account holders can yield significant risk reduction. Treat members as one of your first lines of defense and invest in ongoing educational programs that frequently remind them of good internet hygiene practices and how to spot potential scams. At a minimum, have a dedicated webpage on your site for educational content as well as clear, simple-to-follow instructions on reporting suspicious activity. Consider sending out regular newsletters reminding members about common account takeover tactics and provide security awareness materials in documentation that members are most likely to read, such as new account documents.

- Ensure that your business practices match and do not enable account takeover tactics. For example, make sure that the policy dictates that account login URLs are never sent via email; be sure that policy is well-communicated internally and to your members so they will be more wary of links in emails purporting to be from your institution.

- Have clearly articulated response plans for phishing, vishing, SMiShing, and other attacks that target your members directly. It is critical to respond quickly and decisively to minimize the immediate impact of an attack. The longer an attack is active (phishing site is up, emails distributed, active phone numbers or text messages distributed), the greater the risk of stolen credentials.

- Build relationships with external authorities, service providers, and partners, such as PhishLabs, to support response to attacks. Account takeover attacks typically rely on compromised infrastructure that is managed by legitimate organizations and that infrastructure can be located anywhere in the world. Working with experienced partners with well-established networks will speed mitigation of account takeover attacks.

- Adopt a proactive and offensive anti-fraud strategy. While it’s important to have good controls in place that make it more difficult for cybercriminals to carry out fraud, their effectiveness is limited. Institutions should invest in capabilities for proactively detecting attacks targeting their members and aggressively disrupting the cybercrime systems and tools used against them.

*continued on Page 2*

**Stacy Shelley**
Vice President

PHISHLABS
Prevent. Defend. Fight back.

**Contact Info**
**www.phishlabs.com**
**Phone: 877.227.0790**

**Stacy Shelley** is Vice President at PhishLabs and is responsible for understanding prevailing and emerging security trends and their impact on information security leaders. Mr. Shelley has more than 8 years of experience in the information security industry with tenure at leading security service providers, SecureWorks and LURHQ. Mr. Shelley has frequently spoken on a range of topics spanning network security, web application security, regulatory compliance, and threat intelligence.

CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

# *Meeting the Challenges of Attacks, Breaches & Compliance*

At PhishLabs, we fight back against the cybercriminal's entire ecosystem by detecting, analyzing and proactively dismantling the systems and illicit services used to attack businesses. When a data breach occurs, it can be expected that cybercriminals will deploy tactics such as phishing, vishing or SMiShing to gather additional personally identifiable information that will enable account takeover.

Our services go beyond the usual reactive response to cybercrime threats. Not only do we rapidly shut down malicious URLs to disrupt the current campaign but we also investigate and target the infrastructure beneath the surface that is used to plan, stage, launch and monetize cybercrime attacks. This includes distribution networks, malware/exploit kits, phishing kits, drop sites, money mules, laundering systems, and other aspects of the ecosystem. Proactively shutting down the cybercrime ecosystem increases the costs to the attacker which deters cybercriminals from targeting our clients – the criminals move on to more vulnerable targets that do not fight back.

Sector-wide investments in stronger authentication and fraud monitoring tools to satisfy 2011 FFIEC compliance requirements have not been enough to reverse the growing trend of account takeover attacks. Partnering with PhishLabs offers a dedicated team of security experts that monitor and fight back against security threats on your behalf 24/7, 365 days of the year.

Our account takeover prevention (ATO|Prevent) service is designed specifically for community financial institutions. Using proprietary technology, we analyze millions of suspicious URLs and malware samples every day from service providers, data feeds, security partners, and our own research. When a possible attack is detected, it is quickly confirmed and mitigated by our cybercrime experts. The median time it takes for our experts to shut down attacks is less than 5 hours and we have a 100% success rate in taking down malicious sites, phone numbers, and rogue mobile applications. ATO|Prevent provides detection and mitigation of:

* Phishing emails and websites
* Vishing phone calls
* SMiShing text messages
* Banking Trojans that steal customer credentials and hijack their online banking sessions
* Malicious mobile apps that impersonate your brand
* Distributed-denial-of-service (DDoS) threats

ATO|Prevent facilitates compliance with fraud prevention and DDoS guidance and helps financial institutions go beyond the regulatory checkbox.

**Stacy Shelley**
Vice President

PHISHLABS
Prevent. Defend. Fight back.

**Contact Info**
**www.phishlabs.com**
**Phone: 877.227.0790**

**Stacy Shelley** is Vice President at PhishLabs and is responsible for understanding prevailing and emerging security trends and their impact on information security leaders. Mr. Shelley has more than 8 years of experience in the information security industry with tenure at leading security service providers, SecureWorks and LURHQ. Mr. Shelley has frequently spoken on a range of topics spanning network security, web application security, regulatory compliance, and threat intelligence.