TOOLKIT

Battling Fraudsters

Nicsa explores best practices for battling bad actors in a work-from-home, flex-time environment.

The global asset management industry continues to see unprecedented, widespread, and sophisticated phishing schemes and malware attempts targeting financial institutions and their customers. Elder financial exploitation is heightened, playing on fear and urgency. The following guidance is offered to asset managers and professional service providers as a means to stimulate discussion around industry best practices.

These are just examples of some helpful tips. Individual member firms may have their own specific policies and procedures associated with these topics.

MONITOR AND ADJUST CONTROLS FOR WFH/FLEX TIME

- Adjust cyber controls to fit any work-from-home or flex-time environments. Establish and implement baselines to monitor network activity with flexible work schedules in mind. Adjust to new and different peak volume periods.
- Adjust password reset controls. Ensure that the process is easy and frequent, while leaning toward more aggressive password strength requirements.
- Have mechanisms in place to install patches to every employee's machine promptly and across the employee base.

TRAIN EMPLOYEES ON POTENTIAL SCHEMES

- Train new employees immediately when on-boarded. Make sure they understand the basics and general principles.
- Remind your existing staff to stay diligent and that you are depending on them.
- Evaluate red flags that may be specific to the global pandemic (no callback number provided because “they are ill”, or otherwise “not available”).
- Refresh employees on important technology policies.
- Establish and/or increase phishing tests and training.
- Provide employees with information on how to report suspicious activity. Consider adding a link on your Internet where employees can make reports that go directly to a global security team to investigate and remediate.
- Enhance training to adequately cover all vulnerable areas of the organization. Obvious threats involve client-facing staff, but don’t forget your payments team, for example, who are highly vulnerable for business e-mail compromise (impersonators requesting wires to unknown addresses; attempts to obtain credentials to banking applications).
- Establish additional controls such as secondary approvals for internal requests.