Division of Gaming Enforcement Cyber Security Best Practices

The most prevalent cyber-attack against online Internet gaming providers is credential stuffing. In these attacks, lists of compromised username/password pairs from other websites are used in an automated attempt to log into gaming platforms. These attacks are successful when patrons reuse the same username/password combination on multiple websites. Unfortunately, many patrons do reuse credentials as evidenced by the success of these attacks.

Stopping credential stuffing attacks was discussed in 2021 with all New Jersey casino Information Security Officers, the head of the NJ Office of Homeland Security and Preparedness, along with other law enforcement entities within the State. A survey of all Internet gaming operators was performed to understand existing defenses against credential stuffing.

Credential stuffing is a subset of account takeover attacks, where a threat actor can hijack a patron account. Going forward, the Division has determined that additional security features are required to maintain the highest levels of integrity in the online gaming industry. In order to protect New Jersey patrons from account takeover, all Internet gaming operators shall, at a minimum, implement multi-factor authentication for patron logins.

N.J.A.C. 13:69O-1.1 defines “multi-factor authentication” as a type of strong authentication that uses two of the following to verify a patron's identity:

1. Information known only to the patron, such as a password, pattern or answers to challenge questions;
2. An item possessed by a patron such as an electronic token, physical token or an identification card; or
3. A patron's biometric data, such as fingerprints, facial or voice recognition.

Once a patron has successfully logged in using multi-factor authentication, subsequent logins to the same account on that same device can be exempt from multi-factor authentication for a period not to exceed two weeks.

These plans shall be evaluated and approved by the Division prior to implementation. Division best practice is for the login process not to allow an email address as the username since this is most susceptible to current credential stuffing attacks.

Finally, if you ever discover that a patron’s account on your system is associated with more than three devices in a 24 hour period, the Division expects that you will perform all necessary due diligence to ensure the account is not associated with any fraud.