PRASFAA
Asociación de Administradores
de Asistencia Económica
Estudiantil de Puerto Rico

Comité de Regulaciones Federales y Estatales – Boletín 2018- 49

ELECTRONIC ANNOUNCEMENT

El FSA identificó una campaña de *phishing* maliciosa que puede conducir a posibles fraudes asociados con reembolsos de estudiantes y distribuciones de ayuda.

¿Qué está ocurriendo?: Varias instituciones de educación superior (IHE) informaron que los *hackers* están usando un correo electrónico *phishing* para obtener acceso a las cuentas de los estudiantes a través del portal de estudiantes de IHE (consulte el ejemplo de correo electrónico *phishing* a continuación). La naturaleza de las solicitudes indica que los *hackers* han realizado un cierto nivel de investigación y entienden el uso que hacen las instituciones de los portales y métodos de los estudiantes. Estos ataques son exitosos debido al cumplimiento del estudiante al proporcionar la información solicitada y el uso de solo un factor para la autenticación.

Al obtener acceso al portal, el *hacker* cambia el destino del depósito directo del alumno a una cuenta bancaria controlada por el *hacker*. Como resultado, los reembolsos de *FSA* destinados al estudiante se envían al *hacker*. El FSA cree que los *hackers* están practicando y perfeccionando el esquema en una escala más pequeña ahora y que esto surgirá como una amenaza prominente contra las IHE durante los periodos en que los fondos de la FSA se difunden en grandes volúmenes.

¿Cómo proteger a las Instituciones de Educación Superior?: El FSA recomienda encarecidamente a las IHE que fortalezcan su postura de ciberseguridad mediante el uso de procesos de autenticación de dos factores o de factores múltiples. Estos tipos de autenticación dependen de una combinación de factores, por ejemplo, nombre de usuario y contraseña combinados con un PIN o preguntas de seguridad o acceso a través de un dispositivo seguro y designado.

Si used cree que su institución ha sido víctima de un ataque, informe el incidente de inmediato a cpssaig@ed.gov and FSASchoolCyberSafety@ed.gov. Incluir la información siguiente:

- Nombre de la institución
- Fecha en que ocurrió el incidente (si se conoce)
- Fecha en que se descubrió el incidente
- Copia del correo electrónico de phishing (si está disponible)
- Alcance del impacto (número de estudiantes)

Estado de remediación (lo que se ha hecho desde el descubrimiento)

Punto de contacto de la institución

Para información relacionada a este anuncio electrónico hacer referencia a FSASchoolCyberSafety@ed.gov

Posted Date: August 31, 2018

Author: Federal Student Aid

Subject: Active Phishing Campaign Targeting Student Email Accounts

Federal Student Aid (FSA) has identified a malicious phishing campaign that may lead to potential fraud associated with student refunds and aid distributions.

What is happening: Multiple institutions of higher education (IHEs) have reported that attackers are using a phishing email to obtain access to student accounts via the IHE student portal (see example phishing email below). The nature of the requests indicates the attackers have done some level of research and understand the schools' use of student portals and methods. These attacks are successful due to student compliance in providing requested information and the use of just one factor for authentication.

Upon gaining access to the portal, the attacker changes the student's direct deposit destination to a bank account controlled by the attacker. As a result, FSA refunds intended for the student are sent to the attacker. FSA believes that attackers are practicing and refining the scheme on a smaller scale now and that this will emerge as a prominent threat against IHEs during periods when FSA funds are disseminated in large volumes.

Note: Any funds disbursed inappropriately may become the responsibility of the institution.

Example phishing email:

Why IHEs are vulnerable to this attack: The attackers are exploiting a common practice at many IHEs: the use of single-factor authentication to access institution systems. Single-factor authentication is the simplest method of authentication where a person uses only one credential to verify him or herself online; usually the one credential is a password matched to a username.

How to protect IHEs: FSA strongly encourages IHEs to strengthen their cybersecurity posture through the use of two-factor or multi-factor authentication processes. These types of authentication rely on a combination of factors, for example, username and password combined with a PIN or security questions or access through a secure, designated device.

If you believe your institution has fallen victim to an attack, report the incident immediately to cpssaig@ed.gov and FSASchoolCyberSafety@ed.gov. Include the following:

- Name of the institution
- Date the incident occurred (if known)
- Date the incident was discovered
- Copy of the phishing email (if available)
- Extent of the impact (number of students)
- Remediation status (what has been done since discovery)
- Institution point of contact

Suggested remediation steps if an institution falls victim to the attack:

- Temporarily freeze refund requests until the scope of the incident can be known. Note, refunds must still be provided within regulatory guidelines which may require a change in how impacted IHEs issue refunds, e.g. issue paper checks.
- Temporarily disable changes to direct deposits for refunds.
- Block IP addresses observed in institution logs related to the attack.
- Disable campus credentials or passwords for potentially affected students and require password resets.
- Perform additional forensic analysis on server and application logs from recent weeks.
- Notify all students, warning them of active phishing attempts and encourage them to be vigilant and careful about using links and entering personally identifiable information into websites.

FSA will continue to monitor this situation and will send out additional information as appropriate. That information may include additional examples of the phishing emails, training resources, and best practices about how to avoid falling victim to phishing attacks.

Thank you for your attention to this matter. FSA is committed to working with IHEs to thwart phishing attacks and protect student financial aid information. If you have any questions about the information included in this announcement, please contact FSASchoolCyberSafety@ed.gov.

COMITÉ DE REGULACIONES FEDERALES Y ESTATALES