Data Incident Response

Naviance

Montgomery County Public Schools (MCPS) is notifying you of a data security incident that occurred with Naviance, an online college and career readiness program that supports MCPS students in exploring and developing their postsecondary plans. Certain data elements from Naviance accounts at Wheaton High School were accessed and downloaded by an unauthorized user. Working with Naviance and law enforcement, MCPS immediately took steps to secure the platform and began an investigation to identify the unauthorized user. The threat has now been eliminated and MCPS is implementing improvements to prevent such unauthorized access from happening again. Additional information about the incident, MCPS' actions to address the incident, and information regarding what you can do to protect your personal information is provided below.

MCPS is committed to safeguarding the privacy and security of our students, families, and staff and MCPS sincerely regrets that this incident has occurred. MCPS takes this event very seriously and we will continue to be forthcoming with any relevant information.

What Happened?

Naviance notified MCPS on Friday, October 4, 2019 that a data security incident occurred on Thursday, October 3, 2019 impacting 1,343 Naviance student accounts and one parent/guardian account at Wheaton High School.

On Thursday, October 3, 2019 between 8:10PM and 10:14PM, an unauthorized user performed a sequential brute force attack against Wheaton High School's Naviance platform in order to access user accounts. The unauthorized user attempted many username and password combinations, eventually gaining access to 1,344 accounts. The unauthorized user then downloaded demographic information from the accessed accounts. The information accessed did not include social security numbers, banking information, or credit card information.

At 10:14PM, Naviance discovered the suspicious activity and blocked the IP address of the incoming attacks so that further attempts to access the system were stopped. On Friday, October 4, 2019, Naviance notified MCPS of the incident and provided the necessary information for MCPS to begin an investigation. Naviance immediately reset passwords for the affected users. Affected users will be prompted to set a new password in order to access their Naviance accounts.

What Information Was Involved?

The following chart describes the data elements that Naviance confirms were exposed:

Exposed Data Elements		
Name	Date of Birth	Highest ACT Score
Ethnicity	Grade Level	Highest IB Score
Gender	Student ID #	Student Address
GPA	Weighted GPA	Home Phone #

Email Address	Highest SAT Score	Mobile Phone #
Assigned Counselor	Highest PSAT Score	Nickname

What We Are Doing

Once MCPS was notified of the data security incident, MCPS immediately contacted Naviance to obtain detailed information regarding the attack to assess the exposure of student and parent/guardian information and to determine a course of action. Internally, the Office of the Chief Technology Officer created a cross-office collaborative team including the Department of Systemwide Safety and Emergency Management, the Office of Student and Family Support and Engagement, the Office of School Support and Improvement, the Office of General Counsel, and the Office of Communications.

Based on information provided by Naviance, the MCPS team identified two MCPS students as potential suspects. On Monday, October 7, 2019, MCPS engaged the Montgomery County Police Department (MCPD) to assist with the investigation. Together, MCPS and MCPD successfully identified the student responsible for the brute force attack. The responsible student also indicated that the downloaded data was shared with other students. With cooperation from the student and the student's parents, MCPD took possession of the student's technology devices for further investigation. The student currently faces disciplinary action, as determined by local school administrators, and possible criminal charges. Criminal investigation of this data security incident by MCPD is ongoing.

Furthermore, in addition to the password reset performed by Naviance for affected users, MCPS is initiating a password reset for all Naviance student accounts. School staff will be available to assist students with resetting their passwords. MCPS recognizes the importance of Naviance and will minimize the impact of this incident on coursework and the college application process.

What You Can Do

As with any incident regarding personally identifiable information, there are many precautionary steps that parents/guardians can take to secure their childrens' identity. Recommendations include:

- Request a free credit freeze for your child. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions from each of these credit bureaus: Equifax, Experian, and TransUnion.
- You can check to see if your child has a credit report. Each bureau listed above has specific instructions for these requests. If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove the fraudulent accounts.
- Review information on Child Identity Theft from the Federal Trade Commission.

For More Information

If you have any questions regarding this incident, or if you desire any further information or assistance, please email information_security@mcpsmd.net.

Respuesta a los Datos del Incidente

Naviance

Montgomery County Public Schools (MCPS) les notifica a ustedes sobre un incidente de seguridad de datos que ocurrió con Naviance, un programa en línea de preparación para la universidad y carreras que ayuda a los estudiantes de MCPS a explorar y desarrollar sus planes postsecundarios. Ciertos elementos de información de las cuentas de Naviance en Wheaton High School fueron accedidos y descargados por un usuario no autorizado. Trabajando con Naviance y con las autoridades de cumplimiento de la ley, MCPS inmediatamente tomó medidas para proteger la plataforma e inició una investigación para identificar al usuario no autorizado. El riesgo ya ha sido eliminado y MCPS está implementando mejoras para que dicho acceso no autorizado no vuelva a suceder. A continuación ofrecemos información adicional sobre el incidente, las acciones tomadas por MCPS para tratar el incidente e información sobre lo que ustedes pueden hacer para proteger su información personal.

MCPS está comprometido a resguardar la privacidad y seguridad de nuestros estudiantes, familias y empleados, y MCPS sinceramente lamenta que este incidente haya ocurrido. MCPS toma este hecho muy en serio y continuaremos comunicándoles cualquier información relevante.

¿Qué sucedió?

El viernes, 4 de octubre, 2019, Naviance notificó a MCPS que el jueves, 3 de octubre, 2019, había ocurrido un incidente de seguridad de datos que afectaba a 1,343 cuentas de Naviance de los estudiantes y una cuenta de los padres/guardianes en Wheaton High School.

El jueves, 3 de octubre, 2019, entre las 8:10 p.m. y las 10:14 p.m., un usuario no autorizado efectuó un ataque de fuerza bruta en secuencia contra la plataforma de Naviance de Wheaton High School, con el fin de acceder a las cuentas de los usuarios. El usuario no autorizado intentó con muchas combinaciones de nombres de usuarios y contraseñas, eventualmente consiguiendo acceso a 1,344 cuentas. El usuario no autorizado entonces descargó información demográfica de las cuentas accedidas. La información accedida no incluía números de seguro social, información bancaria o información de tarjetas de crédito.

A las 10:14 p.m., Naviance descubrió la actividad sospechosa y bloqueó la dirección de IP de donde provenían los ataques y por lo tanto intentos subsiguientes de acceder al sistema fueron coartados. El viernes, 4 de octubre, 2019, Naviance notificó a MCPS sobre el incidente y proporcionó la información necesaria para que MCPS iniciara una investigación. Naviance inmediatamente restableció las contraseñas de los usuarios afectados. A los usuarios afectados se les indicará que deberán crear una nueva contraseña para poder acceder a sus cuentas de Naviance.

¿Qué Información Fue Comprometida?

El siguiente cuadro describe los elementos de información que Naviance confirma que fueron expuestos:

Elementos de Información Expuesta		
Nombre	Fecha de Nacimiento	Puntaje de ACT Más Alto
Etnicidad	Grado Académico	Puntaje de IB Más Alto
Género	No. de Estudiante	Domicilio del/de la Estudiante
Promedio de Calificaciones	GPA Ponderado	No. de Teléfono de la Casa

(Grade Point Average–GPA)	(Weighted GPA)	
Correo Electrónico	Puntaje de SAT Más Alto	No. de Teléfono Móvil
Consejero/a Escolar Designado/a	Puntaje de PSAT Más Alto	Apodo

Lo Que Nosotros Estamos Haciendo

Una vez que MCPS recibió notificación del incidente de seguridad de datos, MCPS se contactó de inmediato con Naviance para obtener información detallada sobre el ataque, a fin de evaluar la información de estudiantes y padres/guardianes expuesta y determinar un curso de acción. En el ámbito interno, la Oficina del Jefe de Tecnología (Office of the Chief Technology Officer) creó un equipo colaborativo entre oficinas, incluyendo el Departamento de Administración de Seguridad y Emergencias de Todo el Sistema (Department of Systemwide Safety and Emergency Management), la Oficina de Apoyo y Participación Familiar (Office of Student and Family Support and Engagement), la Oficina de Apoyo y Mejoramiento Escolar (Office of School Support and Improvement), la Oficina de Asuntos Jurídicos (Office of the General Counsel) y la Oficina de Comunicaciones (Office of Communications).

Basado en información suministrada por Naviance, el equipo de MCPS identificó a dos estudiantes de MCPS como probables sospechosos. El lunes, 7 de octubre, 2019, MCPS involucró al Departamento de Policía del Condado de Montgomery (Montgomery County Police Department–MCPD) para que asistiera en la investigación. Juntos MCPS y MCPD identificaron exitosamente al estudiante responsable del ataque de fuerza bruta. El estudiante responsable también indicó que los datos descargados fueron compartidos con otros estudiantes. Con la cooperación del estudiante y los padres del estudiante, MCPS tomó posesión de los dispositivos tecnológicos del estudiante para más investigación. El estudiante actualmente se enfrenta a acción disciplinaria, según lo determinen los administradores de la escuela local, y posibles cargos penales. La investigación criminal de MCDP sobre este incidente de seguridad de datos está en curso.

Por otra parte, además del restablecimiento de contraseñas efectuado por Naviance para los usuarios afectados, MCPS está iniciando un restablecimiento de contraseñas para todas las cuentas de Naviance de los estudiantes. El personal escolar estará a disposición para ayudar a los estudiantes a cambiar sus contraseñas. MCPS reconoce la importancia de Naviance y minimizará el impacto de este incidente en el trabajo de curso y en el proceso de solicitud universitaria.

Lo Que Usted Puede Hacer

Como en el caso de cualquier incidente relacionado con información personalmente identificable, existen muchas medidas de precaución que los padres/guardianes pueden tomar para proteger la identidad de sus hijos. Las recomendaciones incluyen:

- Solicitar congelación de crédito gratuita para su hijo/a. Una congelación de crédito dificultará que alguien use la información de su hijo/a para abrir cuentas. Para efectuar una congelación, siga las instrucciones específicas de cada una de estas agencias de informes de crédito: Equifax, Experian y TransUnion.
- Usted puede chequear para ver si su hijo/a tiene un reporte de crédito. Cada agencia listada arriba tiene instrucciones específicas para este tipo de pedido. Si una agencia de información de crédito tiene un reporte de crédito para su hijo/a, la agencia le enviará una copia del reporte. Use las instrucciones incluidas con el reporte de crédito para eliminar cuentas fraudulentas.

- Revise la información sobre Robo de Identidad Infantil (Child Identity Theft) de la Comisión Federal de Comercio (Federal Trade Comission).

Para Más Información

Si usted tiene cualquier pregunta relacionada con este incidente, o si desea más información o asistencia, por favor envíe un correo electrónico a information_security@mcpsmd.net.