Cuentas y claves

365 MFA. Doble factor de validación

Cuentas comprometidas

Son cuentas cuyas credenciales han sido capturadas y son utilizadas fraudulentamente por *hackers* para lanzar campañas de *phishing* que afectan a los correos de la plataforma 365 Educación.

Muchos de los casos de *phishing* se producen por usos inadecuados de las cuentas educativas por parte de sus usuarios o usuarias. Para evitarlo se recuerda que **NO se deben utilizar las cuentas educativas para usos ajenos a educación, especialmente para registrarse en plataformas como webs poco fiables, redes sociales, juegos, concursos, comercio online, etc.**

En la siguiente guía se recogen indicaciones para reconocer este tipo de correos, para saber cómo actuar si se sospecha que un correo es fraudulento y algunas cuestiones generales sobre la protección de las credenciales y los dispositivos. Se recomienda encarecidamente su lectura y difusión en el centro, especialmente entre el alumnado.

Guía. Correos fraudulentos

Medidas de seguridad sobre cuentas comprometidas

Dado que las cuentas educativas son cuentas institucionales del Principado, desde la Consejería de Educación y desde la DG de Estrategia Digital e Inteligencia Artificial del Principado se toman una serie de medidas de seguridad para proteger la plataforma 365 y a sus usuarios y usuarias, evitando en lo posible la proliferación de este tipo de mensajes fraudulentos dentro de la organización 365 Educación.

Diariamente se monitorizan los envíos masivos de correo para detectar campañas de *phishing* y se toman de oficio las siguientes medidas de seguridad:

- Se filtran los correos catalogados como *phishing* y se eliminan de las bandejas de entrada de todas las cuentas de 365 Educación. No obstante, es posible que algún usuario o alguna usuaria vea estos correos si todavía no están indexados o si lo hace antes de su eliminación masiva.

- Se cambia de inmediato la contraseña de la cuenta comprometida.
- Se cierran las sesiones abiertas en todos los dispositivos del usuario o de la usuaria.
- Se borran las reglas de bandeja de entrada del buzón de correo para evitar que los *hackers* las utilicen para conseguir mayor difusión de correos fraudulentos dentro de la plataforma. El usuario o la usuaria podrá volver a crearlas cuando recupere la cuenta.
- **Se aplica el sistema MFA de doble factor de validación** cuando Microsoft considera la **cuenta en riesgo,** normalmente por actividad fraudulenta, ataques desde el extranjero, etc.

Qué es el doble factor de validación (MFA)

Cuando una cuenta está en situación de riesgo, la política de seguridad del Principado y de Microsoft puede asignar a la cuenta comprometida una **doble validación** en cada acceso a la plataforma. Ya no bastará con poner usuario y contraseña al acceder a 365, sino que el sistema pedirá un segundo código de validación que se obtiene a través del móvil asociado a la cuenta, configurado previamente.

Infografía. Qué es MFA (pdf)

Guía. Activación MFA (pdf)

Responsabilidad

Las cuentas educativas son cuentas institucionales del Principado y están sujetas a sus políticas y normativa de seguridad y protección de datos. La persona titular de la cuenta queda obligada a respetar las condiciones de uso de los servicios que utilice (se asumen en cada acceso), a desarrollar buenas prácticas de uso que respeten los servicios públicos colectivos y a cumplir la normativa de aplicación en cada caso. Los usos inadecuados pueden derivar en perjuicios para el propio usuario o la propia usuaria (bloqueos, aplicación de MFA, pérdidas de información…), para otros usuarios u otras usuarias o para la integridad de las plataformas educativas.

Las cuentas educativas NO deben utilizarse para usos ajenos a Educación. El usuario o la usuaria de una cuenta educativa deberá abstenerse de utilizarla para registrarse en plataformas ajenas, especialmente cuando se trata de webs poco fiables, redes sociales, juegos, concursos, comercio online, etc.

Más información

Servicios educativos - Información cuentas educativas - Sistema cl@ve – CGSI: https://itsmasturias.service-now.com/ - 985109300 – Ext. 19300