GOBIERNO DEL PARAGUAY | MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GUÍA DE CIBERSEGURIDAD
PARA DOCENTES

ENERO 2025

ÍNDICE

Introducción **2**
¿Por qué los docentes pueden ser objetivo de ciberdelincuentes? **3**
Principales Amenazas para Docentes **3**
1. Ingeniería Social 3
1.1. Phishing 3
1.2. Pretexting 4
1.3. Baiting 5
2. La protección de datos y la privacidad 6
3. Uso de Dispositivos y Redes 7
4. Manejo de Material Educativo y Recursos Digitales 7
5. Ataques de Ransomware 8
6. Malware en Dispositivos Personales 8
7. Suplantación de Identidad en Redes Sociales 9
Conclusión **10**

Introducción

El avance tecnológico ha transformado la educación, brindando herramientas innovadoras, pero también ha generado riesgos en el ámbito digital. La ciberseguridad se ha vuelto esencial para proteger la información personal de docentes y estudiantes. Los docentes, debido a su rol y acceso a sistemas, son objetivos atractivos para los ciberdelincuentes.

El CERT-PY ofrece una guía para que los docentes fortalezcan su seguridad digital, abordando amenazas comunes y estrategias para protegerse, como la seguridad de datos personales, el uso seguro de dispositivos, redes y la protección de material educativo. También se enfoca en prevenir ataques de ransomware y fomentar una cultura de ciberseguridad entre estudiantes.

El papel del docente va más allá de la enseñanza; también deben guiar a sus alumnos en el uso responsable de la tecnología. Esta guía busca ser un recurso útil para enfrentar los desafíos del mundo digital y garantizar un entorno educativo seguro.

¿Por qué los docentes pueden ser objetivo de ciberdelincuentes?

Los docentes suelen ser un objetivo atractivo para los ciberdelincuentes por varias razones:

- **Información valiosa**: Los docentes tienen acceso a una gran cantidad de información confidencial, tanto propia como de sus alumnos, incluyendo datos personales, calificaciones, información médica y más.
- **Acceso a sistemas**: Los docentes suelen tener acceso a sistemas informáticos de las instituciones educativas, lo que les da a los delincuentes una vía para acceder a información aún más valiosa.
- **Confianza**: Los docentes suelen ser personas confiadas y bien intencionadas, lo que los hace más susceptibles a los ataques de ingeniería social.

Principales Amenazas para Docentes

1. Ingeniería Social

La ingeniería social es un conjunto de técnicas que utilizan los delincuentes para manipular a las personas y obtener información confidencial o acceso a sistemas. Los ataques de ingeniería social se basan en la confianza y en la manipulación psicológica de las víctimas.

Los docentes, como cualquier otro individuo, pueden ser víctimas de esta técnica y es crucial que estén al tanto de como protegerse.

¿Cómo funciona la ingeniería social ?

Los ataques pueden variar, pero algunos ejemplos comunes incluyen:

- **Phishing: Correos** electrónicos o mensajes con enlaces maliciosos o archivos adjuntos que, al ser abiertos, pueden infectar sus dispositivos o robar sus credenciales.
- **Pretexting:** Un escenario inventado para ganarse la confianza del docente y obtener información sensible bajo un pretexto convincente.
- **Baiting:** Ofrecer algo atractivo (como un recurso educativo gratuito) para atraer al docente a una trampa y robar sus datos.

1.1. Phishing

El phishing es una de las formas más comunes de ingeniería social. Los atacantes envían correos electrónicos o mensajes de texto haciéndose pasar por entidades legítimas (como bancos, plataformas educativas o incluso colegas) para engañar a los docentes y obtener información confidencial.

¿Cómo funciona?

- El atacante envía un correo electrónico o mensaje de texto con un enlace malicioso o un archivo adjunto infectado.
- El mensaje suele generar una sensación de urgencia (por ejemplo, "Tu cuenta ha sido bloqueada") para que el docente actúe sin pensar.
- Si el docente hace clic en el enlace o abre el archivo, puede ser redirigido a una página web falsa que imita la de una entidad legítima, donde se le pedirá que ingrese sus credenciales (nombre de usuario y contraseña).
- Una vez que el docente ingresa sus credenciales, el atacante las captura y puede utilizarlas para acceder a su cuenta de correo electrónico, plataforma educativa u otros sistemas.

Señales de alerta:

1. El mensaje contiene errores de ortografía o gramática.
2. El mensaje solicita información personal o credenciales de acceso.
3. El mensaje genera una sensación de urgencia o amenaza.
4. El enlace o archivo adjunto parece sospechoso (por ejemplo, tiene una extensión extraña o un nombre poco claro).
5. El remitente del mensaje es desconocido o no confiable.

Recomendaciones:

- No abrir enlaces ni descargar archivos adjuntos de mensajes sospechosos.
- Verificar la dirección de correo electrónico del remitente antes de responder.
- No ingresar credenciales de acceso en páginas web sospechosas.
- Activar la autenticación de dos factores en cuentas importantes.
- Mantener el software antivirus actualizado.

5.1. Pretexting

El pretexting implica crear un escenario falso para ganarse la confianza del docente y obtener información sensible. El atacante puede hacerse pasar por un colega, un técnico de soporte o incluso un padre de alumno.

¿Cómo funciona?

- El atacante contacta al docente por teléfono, correo electrónico o mensaje de texto, inventando una historia convincente.

- El pretexto puede ser una solicitud de ayuda técnica, una consulta sobre un alumno o cualquier otra situación que parezca legítima.
- El objetivo es obtener información personal del docente, como contraseñas, datos de acceso a plataformas educativas o información sobre alumnos.

Señales de alerta:

1. La persona que contacta al docente es desconocida o no identificada.
2. La historia que cuenta parece poco creíble o sospechosa.
3. La persona solicita información personal que no debería necesitar.
4. El docente se siente incómodo o presionado para dar información.

Recomendaciones:

- Desconfiar de las solicitudes inesperadas de información personal.
- Verificar la identidad de la persona que contacta al docente antes de dar cualquier información.
- No compartir contraseñas ni datos de acceso con nadie.
- Si tienes dudas, contacta directamente a la persona o entidad que supuestamente está contactando al docente.

5.2. Baiting

El baiting utiliza una carnada atractiva para atraer al docente a una trampa. La carnada puede ser un recurso educativo gratuito, un descuento exclusivo o cualquier otra cosa que sea de interés para el docente.

¿Cómo funciona?

- El atacante publica un anuncio o envía un mensaje ofreciendo una carnada atractiva.
- El docente, atraído por la oferta, hace clic en el enlace o descarga el archivo adjunto.
- El enlace o archivo adjunto puede contener malware que infecta el dispositivo del docente o roba sus datos.

Señales de alerta:

1. La oferta parece demasiado buena para ser verdad.
2. El enlace o archivo adjunto proviene de una fuente desconocida o no confiable.
3. El sitio web al que se redirige al docente parece sospechoso o poco profesional.

Recomendaciones:

- Desconfiar de las ofertas demasiado buenas para ser verdad.
- No hacer clic en enlaces ni descargar archivos adjuntos de fuentes desconocidas o no confiables.
- Verificar la reputación del sitio web antes de ingresar cualquier información personal.

La protección de datos y la privacidad

Son aspectos críticos en el entorno digital actual, especialmente en el ámbito educativo donde se maneja información sensible de docentes y alumnos. La exposición de esta información puede tener consecuencias graves, como el robo de identidad y fraudes.

Datos que pueden estar en riesgo

1. **Datos personales de docentes:**
   - Información de contacto (nombre, dirección, teléfono, correo electrónico).
   - Datos laborales (historial profesional,cargo, salario).
   - Información financiera (cuentas bancarias, tarjetas de crédito).
   - Datos de acceso a plataformas educativas y otros servicios en línea.
2. **Datos personales de alumnos:**
   - Información de contacto (nombre, dirección, teléfono, correo electrónico de los padres).
   - Datos académicos (calificaciones, historial académico, información sobre necesidades educativas especiales).
   - Información médica (alergias, condiciones médicas).
   - Datos de acceso a plataformas educativas.

Cómo se produce la exposición de datos

- **Plataformas educativas:** Algunas plataformas pueden no tener medidas de seguridad adecuadas, lo que facilita el acceso no autorizado a la información.
- **Redes sociales:** Compartir información personal en redes sociales puede exponer a los docentes y alumnos a riesgos de robo de identidad o acoso en línea.
- **Correos electrónicos:** Los correos electrónicos pueden ser interceptados por terceros, especialmente si se utilizan redes Wi-Fi públicas o contraseñas débiles.
- **Dispositivos personales:** Si los dispositivos personales de los docentes o alumnos no están protegidos con contraseñas y software de seguridad, pueden ser vulnerables a ataques de malware que permitan el acceso a la información.

Qué consecuencias puede tener la exposición de datos

- **Robo de identidad:** Los delincuentes pueden utilizar la información personal para abrir cuentas bancarias, solicitar préstamos o realizar compras a nombre de la víctima.
- **Fraudes:** La información financiera puede ser utilizada para realizar compras fraudulentas o retirar dinero de cuentas bancarias.
- **Acoso en línea:** La información personal puede ser utilizada para acosar o intimidar a docentes o alumnos en línea.
- **Daño a la reputación:** La divulgación de información personal sensible puede dañar la reputación de docentes y alumnos.

Cómo proteger los datos y la privacidad

- **Configurar la privacidad en plataformas educativas y redes sociales:** Asegurarse de que la información personal sólo sea visible para las personas autorizadas.
- **Evitar compartir datos personales en foros abiertos o grupos de mensajería sin control:** La información compartida en estos espacios puede ser accesible para cualquier persona.
- **Utilizar contraseñas seguras y diferentes para cada plataforma:** Las contraseñas deben ser difíciles de adivinar y no deben repetirse en diferentes servicios.
- **Mantener el software actualizado:** Las actualizaciones de software suelen incluir parches de seguridad que protegen contra vulnerabilidades conocidas.
- **Instalar un antivirus confiable:** El software antivirus puede detectar y eliminar malware que pueda poner en riesgo la información personal.
- **Cifrar la información sensible:** El cifrado protege la información al convertirla en un formato ilegible para personas no autorizadas.
- **Educar a los alumnos sobre la importancia de la privacidad en línea:** Enseñarles a no compartir información personal con desconocidos y a proteger sus contraseñas.

Uso de Dispositivos y Redes

Los dispositivos electrónicos usados para enseñar pueden ser atacados si no están protegidos.

Recomendaciones:

- Mantener actualizados el sistema operativo y las aplicaciones.
- Instalar un antivirus confiable y evitar descargar programas de sitios no oficiales.
- No usar redes Wi-Fi públicas para acceder a información sensible.

Manejo de Material Educativo y Recursos Digitales

El contenido creado por los docentes (presentaciones, exámenes, etc.) puede ser robado o manipulado.

Recomendaciones:

- Hacer copias de seguridad periódicas de los documentos en la nube y dispositivos externos.
- Usar herramientas de cifrado para proteger información importante.
- Limitar los permisos de acceso a documentos compartidos en plataformas educativas.

Ataques de Ransomware

El ransomware es un tipo de malware que cifra los archivos de un dispositivo o red, impidiendo el acceso a ellos. Los atacantes suelen exigir un rescate para devolver el acceso a los archivos. Los docentes pueden ser víctimas de ransomware si sus dispositivos se infectan con este malware, lo que puede resultar en la pérdida de información importante, como planes de clase, evaluaciones o datos de estudiantes.

Recomendaciones:

- Mantener el software actualizado, incluyendo el sistema operativo, las aplicaciones y el antivirus.
- No abrir correos electrónicos ni descargar archivos adjuntos de remitentes desconocidos.
- No hacer clic en enlaces sospechosos o anuncios en línea.
- Realizar copias de seguridad periódicas de los archivos importantes en un lugar seguro, como un disco duro externo o la nube.
- Considerar la posibilidad de utilizar un software de seguridad que incluya protección contra ransomware.

Malware en Dispositivos Personales

Los dispositivos personales de los docentes, como laptops o teléfonos móviles, también pueden ser blanco de malware. Si estos dispositivos se utilizan para acceder a información relacionada con el trabajo, como cuentas de correo electrónico o plataformas educativas, el malware puede poner en riesgo tanto la información personal como la profesional del docente.

Recomendaciones:

- Instalar un antivirus confiable en todos los dispositivos personales y mantenerlo actualizado.

- No descargar aplicaciones de fuentes no confiables.
- No hacer clic en enlaces o anuncios sospechosos.
- Mantener el sistema operativo y las aplicaciones actualizadas.
- Utilizar contraseñas seguras y diferentes para cada cuenta.

Suplantación de Identidad en Redes Sociales

Los perfiles de redes sociales de los docentes pueden ser objetivo de suplantación de identidad. Los atacantes pueden crear perfiles falsos utilizando la información y fotos del docente para engañar a otras personas, como estudiantes o colegas. Esto puede dañar la reputación del docente y generar confusión o problemas.

Recomendaciones:

- Configurar la privacidad de las redes sociales para limitar quién puede ver la información del perfil.
- No aceptar solicitudes de amistad de personas desconocidas.
- Denunciar cualquier perfil falso que se encuentre.
- Monitorear la actividad en las redes sociales para detectar cualquier comportamiento sospechoso.

Conclusión

Esta guía ha explorado algunas de las amenazas más comunes que enfrentan los docentes en el ámbito de la ciberseguridad.

Es fundamental recordar que el mundo digital evoluciona constantemente y, con él, las amenazas a la ciberseguridad. Los docentes deben ser conscientes de que existen muchas otras amenazas además de las aquí mencionadas. Por lo tanto, es crucial que se informen permanentemente sobre las últimas tendencias en ciberseguridad y que adopten medidas proactivas para protegerse a sí mismos y a sus estudiantes.

El rol del docente en la educación digital va más allá de la transmisión de conocimientos. Los docentes son modelos a seguir para sus alumnos y tienen la responsabilidad de promover un uso seguro y responsable de la tecnología. Al seguir buenas prácticas de ciberseguridad, los docentes no solo protegen su información personal, sino que también contribuyen a crear un entorno de aprendizaje seguro y protegido para sus estudiantes.

La ciberseguridad es una responsabilidad compartida que requiere la participación de todos. Al trabajar juntos, docentes, alumnos, padres y autoridades educativas pueden crear un entorno digital más seguro y protegido para todos.

Fuente:

- https://cybersecuritynews.es/estrategias-de-seguridad-para-docente
- https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educacion.pdf
- https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/guia-para-madres-padres-docentes-amenazas-internet