PRETEXTING: un riesgo silencioso para la seguridad digital

En la era digital, la seguridad y la privacidad son temas que nos afectan a todos. Sin embargo, a menudo se subestiman las técnicas utilizadas por ciberdelincuentes para acceder a nuestra información personal. Una de las tácticas más comunes, pero menos conocidas, es el *pretexting.*

¿QUÉ ES EL PRETEXTING?

El *pretexting* es una forma de ingeniería social en la que **un atacante se hace pasar por alguien de confianza para obtener información sensible de una víctima.** A diferencia de otros métodos de ataque más directos, como el *phishing*, el *pretexting* se basa en la creación de una historia convincente o pretexto para ganarse la confianza de la persona objetivo.

Este engaño puede tomar diversas formas: el atacante puede hacerse pasar por un compañero de trabajo, un representante de una empresa, o incluso un funcionario público. La clave del éxito radica en la construcción de una narrativa lo suficientemente creíble como para que la víctima revele datos confidenciales, como números de tarjeta de crédito, claves de acceso, o incluso información personal como direcciones y fechas de nacimiento.

EL IMPACTO DEL PRETEXTING

Aunque el *pretexting* puede parecer una táctica inofensiva a simple vista, sus consecuencias pueden ser devastadoras. **Los delincuentes pueden utilizar la información obtenida para cometer fraudes financieros, robar identidades o incluso llevar a cabo actos de espionaje empresarial**.

La preocupación no es solo para las grandes empresas, sino también para individuos que, en su vida cotidiana, podrían caer en esta trampa. La pérdida de datos personales puede abrir la puerta a una serie de delitos como el robo de identidad y, en muchos casos, a la pérdida de dinero.

¿CÓMO PROTEGERSE DEL PRETEXTING?

La prevención del *pretexting* requiere tanto de una actitud vigilante como de una educación constante sobre las técnicas utilizadas por los atacantes. Algunos consejos clave para protegerse incluyen:

- **Verificar siempre las fuentes**: si alguien te solicita información personal, es crucial verificar su identidad. Llama a la empresa o institución de la que supuestamente proviene la solicitud antes de compartir cualquier tipo de dato.
- **Desconfía de las solicitudes urgentes**: los pretextos a menudo incluyen una urgencia para que actúes rápidamente. Si te piden información de forma apresurada, es una señal de alarma.
- **Cuidado con los detalles personales**: los ciberdelincuentes pueden usar incluso la información más trivial sobre ti para hacer que su pretexto sea más convincente. Mantén tu información personal lo más privada posible.
- **Usa la autenticación de dos factores:** siempre que sea posible, activa la autenticación de dos factores en tus cuentas para añadir una capa extra de seguridad.
- **Educación constante**: mantente al tanto de las nuevas amenazas y tácticas utilizadas por los ciberdelincuentes. Participa en programas de formación sobre seguridad cibernética.