¿Qué conoce hasta ahora? - Técnicas de ingeniería social

Instrucciones

"¿Qué conoce hasta ahora?" es un tipo de actividad en la que le solicitamos que simplemente adivine. No se pretende evaluar sus conocimientos. Como recibirá información adicional sobre las respuestas que escoja, estas actividades también le ayudan a aprender.

Arrastre la técnica de ingeniería social que mejor coincida con el texto de la situación.

Simulación de identidad

Carnada

Pretextos

Inspección de basura

Suplantación de identidad (phishing)

Técnica de ingeniería social	Situación	Comentarios
	Encontró una unidad USB en el estacionamiento y la insertó en su equipo portátil. Sin saberlo, instaló así malware en su equipo.	Con esta técnica de ingeniería social, el atacante abandona una unidad flash infectada en un lugar público (por ej., un baño de la empresa), con la expectativa de que alguien desprevenido la introduzca en su equipo portátil corporativo y así instale sin saberlo el malware.
	Un atacante acaba de conseguir en un cesto copias impresas de archivos de configuraciones antiguas de dispositivos.	Con esta técnica de ingeniería social, el atacante hurga en la basura en busca de documentos confidenciales o medios antiguos de almacenamiento.
	Una persona que afirma ser de mantenimiento de calefacción y ventilación le pide pasar a un área protegida.	Con esta técnica de ingeniería social, el atacante finge ser una persona que no es (por ejemplo, un empleado nuevo, un colega, un proveedor, un empleado de una empresa asociada, etc.) para ganarse la confianza de la víctima.
	Recibió un correo electrónico de su banco donde se indica que su cuenta está en peligro y que debe hacer clic en un enlace para rectificar el problema. Al hacer clic, instala sin saberlo malware en el dispositivo.	Con esta técnica de ingeniería social, el atacante envía un mensaje fraudulento que parece ser de una fuente legítima y confiable, para hacer que el destinatario instale malware o revele información personal o financiera.
	Su "banco" lo llama para decirle que su cuenta corre peligro y que les gustaría confirmar su identidad solicitando sus datos personales y financieros.	Con esta técnica de ingeniería social, el atacante finge necesitar información personal o financiera para confirmar la identidad de la persona.

LIVEWORKSHEETS