Taller de ciberseguridad para todos: guía del facilitador

Todo lo necesario para dictar un taller de 45–60 minutos basado en el libro *Guía de Seguridad de un Hacker* de César Cerrudo. No hace falta ser experto en seguridad: la presentación, esta guía y los materiales hacen el trabajo pesado.

01 Para quién es este kit

Equipos de RRHH y seguridad de empresas, docentes y directivos de instituciones educativas, áreas de prevención de fraude de bancos, bibliotecas y organizaciones comunitarias. El taller está pensado para **público general adulto sin conocimientos técnicos**; existe una variante para padres (ver sección 5).

02 Contenido del kit

ARCHIVO	QUÉ ES	USO
Presentación (.pptx)	30 diapositivas con notas de orador en cada una: qué decir, dónde pausar, qué preguntar a la sala.	Proyectar
Guía del facilitador	Este documento: agenda, consejos y preguntas frecuentes.	Leer antes
Hoja de actividades	2 páginas imprimibles: detección de señales, checklist personal y compromiso de acción.	Imprimir 1 por asistente
8 infografías (.pdf)	Material de entrega por tema: phishing, contraseñas, celular, hogar, identidad, familia, respuesta, viajes.	Imprimir o enviar después
Academia online	Lecciones y evaluaciones interactivas para continuar después del taller.	Compartir el enlace
Simulador y test	"¿Real o trampa?" y "¿Qué tan hackeable sos?": prácticas online de 2–10 minutos.	Compartir el enlace

03 Requisitos y preparación

- **Sala:** proyector o pantalla, 45–60 minutos, grupos de 5 a 60 personas.
- **Impresiones:** una hoja de actividades por asistente; opcionalmente las infografías más relevantes para su audiencia (en empresas: 01, 02, 03 y 07; en colegios: 06; en bancos: 01, 02 y 05).
- **Antes del taller:** recorra la presentación una vez leyendo las notas de orador (vista "Presentador" de PowerPoint). Cada nota indica el objetivo de la diapositiva y cómo trabajarla.
- **Regla de oro del facilitador:** el taller alterna miedo y solución. Nunca termine un bloque en la amenaza: cada sección cierra con acciones concretas — respete ese orden.

04 Agenda sugerida (50 minutos)

TIEMPO	DIAPOS.	BLOQUE	CLAVE DE FACILITACIÓN
0–7 min	1–7	**Apertura.** El valor de tu vida digital, hackers vs. criminales, el mapa de las 5 puertas.	En la diapositiva 2, pida que saquen el celular y lo miren: el ejercicio físico engancha. La 7 es el mapa: anúncielo como promesa ("al final van a saber cerrar las cinco").
7–15 min	8–11	**Puerta 1: engaños.** El mail trampa, el test faceb00k, cómo manipulan, el protocolo.	En la 9, pregunte en voz alta cuál dirección es la falsa y espere respuestas antes de revelar. La pausa posterior es el momento más importante del taller.
15–21 min	12–14	**Puerta 2: contraseñas.** El efecto dominó y la escalera hasta las passkeys.	La pregunta de la 12 ("¿usás la misma contraseña?") es retórica: no pida manos levantadas, el humor de la diapositiva hace el trabajo.
21–28 min	15–18	**Puerta 3: el celular.** El robo minuto a minuto, los 4 candados, USB y QR.	La línea de tiempo de la 16 se lee lento, marca por marca. La 17 es accionable: sugiera configurar el PIN de la SIM esa misma tarde.
28–34 min	19–21	**Puerta 4: el hogar.** Router, IoT y la regla de los dos lugares.	"La cámara que te mira" (20) suele generar preguntas: las respuestas están en la sección 6 de esta guía.
34–41 min	22–24	**Puerta 5: la familia.** Grooming, sexting, acompañar en lugar de prohibir.	Baje la voz en la 22 y no apure la 23: es el pico emocional. Pase rápido a la 24 — nunca deje a padres en el miedo sin herramientas.
41–46 min	25–28	**Plan B + IA.** Qué hacer si ya pasó, el error ilegal, deepfakes.	La 26 sorprende (contratar un "hacker" es delito propio): déjela respirar.
46–50 min	29–30	**Cierre + actividad.** El plano completo, "una puerta hoy", hoja de actividades.	Reparta la hoja de actividades y cierre con la Actividad 3 (el compromiso escrito): pedir una sola acción multiplica la ejecución.

VERSIÓN CORTA (25 MINUTOS)

Use las diapositivas 1–2, 7–11, 12–14, 22–24 y 29–30 (apertura, engaños, contraseñas, familia y cierre). Son las secciones de mayor impacto por minuto para audiencias generales.

05 Las tres actividades de la hoja

Actividad 1 — "Cazá las señales" (5 min, durante o después de la Puerta 1)

Cada asistente marca con lapicera las señales de engaño en un correo impreso en la hoja. Son **cinco**: (1) el dominio del remitente no es el oficial ("tubanco-avisos.net"), (2) la urgencia de 24 horas, (3) el pedido de usuario y contraseña, (4) el enlace acortado, y (5) el premio inesperado al pie. Corrija en voz alta: cada señal encontrada en grupo vale más que diez explicadas.

Actividad 2 — "Mis 10 candados" (3 min, hacia el cierre)

Checklist personal de hábitos. No se entrega ni se comparte: es un espejo individual. Sugiera que cada uno cuente sus casilleros vacíos — ese número es su lista de tareas de la semana.

Actividad 3 — "Mi primera puerta" (2 min, cierre del taller)

Cada asistente escribe **una sola acción** y **cuándo** la va a hacer ("hoy a la noche activo el PIN de la SIM"). La evidencia sobre intenciones de implementación es clara: escribir el cuándo duplica la probabilidad de ejecución. Cierre el taller leyendo dos o tres en voz alta, con permiso.

06 Adaptaciones por audiencia

AUDIENCIA	AJUSTES RECOMENDADOS
Empresas	Enfatice las Puertas 1 a 3 y el Plan B. Conecte con políticas internas (reporte de incidentes, MFA corporativo). Entregue las infografías 01, 02, 03 y 07.
Colegios (a padres)	Duplique el tiempo de la Puerta 5 (diapositivas 22–24) y reparta la infografía 06. Para clases CON ALUMNOS no use esta presentación: el kit incluye dos versiones escolares dedicadas ("Guardianes de Internet" 8–12 y "Modo Defensa" 12–15), cada una con su guía docente y hoja de actividades propias.
Bancos (a clientes)	Enfatice Puertas 1 y 2 más la infografía 05 (robo de identidad y dinero). Refuerce el mensaje "el banco nunca pide claves por mensaje" con los canales oficiales propios.
Adultos mayores	Versión corta (25 min), más pausada. Insista en dos reglas: nada de datos por mensaje, y verificar llamando a un familiar de confianza ante cualquier pedido de dinero.

07 Preguntas frecuentes del público (y cómo responderlas)

"¿LOS GESTORES DE CONTRASEÑAS SON SEGUROS? ¿Y SI HACKEAN AL GESTOR?"

Ningún sistema es infalible, pero el gestor con una clave maestra fuerte y MFA es muy superior a la alternativa real: contraseñas repetidas o anotadas. La comparación correcta no es contra la perfección sino contra lo que la persona hace hoy.

"YO NO TENGO NADA QUE OCULTAR / NADIE ME VA A ATACAR A MÍ."

Los ataques actuales son masivos y automáticos: no eligen víctimas, barren. Y todos tenemos algo que perder: la plata de la cuenta, la identidad (con la que pueden endeudarte o delinquir en tu nombre) y el acceso a fotos y conversaciones propias y de terceros.

"¿QUÉ ANTIVIRUS / GESTOR / MARCA ME RECOMENDÁS?"

El taller recomienda categorías y hábitos, no marcas: tiendas oficiales, opiniones, cantidad de descargas y permisos razonables son los criterios para elegir cualquier producto. Evite recomendar marcas puntuales salvo política institucional propia.

"ME PASÓ ALGO PARECIDO, ¿QUÉ HAGO CON MI CASO?"

No analice casos personales en público. Indique el protocolo general (evidencia, denuncia en policía o fiscalía, cambio de contraseñas, canales oficiales) y derive a una conversación privada o a un especialista.

"¿LA IA NO HACE QUE TODO ESTO SEA INÚTIL?"

Al revés: la IA hace los engaños más creíbles, pero las defensas del taller no dependen de detectar errores de redacción sino de hábitos estructurales — verificar por otro canal, no entregar datos por mensaje, MFA. Esos sobreviven a los deepfakes.

08 Checklist del facilitador

- [ ] Recorrí la presentación completa leyendo las notas de orador.
- [ ] Imprimí una hoja de actividades por asistente (y las infografías elegidas).
- [ ] Probé el proyector y la vista de presentador.
- [ ] Tengo a mano los enlaces de la academia, el simulador y el test para compartir al cierre.
- [ ] Sé cuál es mi versión (completa 50 min / corta 25 min) y mi adaptación de audiencia.