Oficina de cibersegurança para todos: guia do facilitador

Tudo o que você precisa para conduzir uma oficina de 45–60 minutos baseada no livro *Guia de Segurança de um Hacker*, de César Cerrudo. Não é preciso ser especialista em segurança: a apresentação, este guia e os materiais fazem o trabalho pesado.

01 Para quem é este kit

Equipes de RH e segurança de empresas, professores e gestores de instituições de ensino, áreas de prevenção a fraudes de bancos, bibliotecas e organizações comunitárias. A oficina foi pensada para **público geral adulto sem conhecimentos técnicos**; existe uma variante para pais (ver seção 5).

02 Conteúdo do kit

ARQUIVO	O QUE É	USO
Apresentação (.pptx)	30 slides com notas do apresentador em cada um: o que dizer, onde pausar, o que perguntar ao público.	Projetar
Guia do facilitador	Este documento: agenda, dicas e perguntas frequentes.	Ler antes
Folha de atividades	2 páginas para imprimir: detecção de sinais, checklist pessoal e compromisso de ação.	Imprimir 1 por participante
8 infográficos (.pdf)	Material de apoio por tema: phishing, senhas, celular, casa, identidade, família, resposta, viagens.	Imprimir ou enviar depois
Academia do Hacker	Lições e avaliações interativas para continuar depois da oficina.	Compartilhar o link
Simulador e teste	"Real ou golpe?" e "Quão hackeável você é?": práticas online de 2–10 minutos.	Compartilhar o link

03 Requisitos e preparação

- **Sala:** projetor ou tela, 45–60 minutos, grupos de 5 a 60 pessoas.
- **Impressões:** uma folha de atividades por participante; opcionalmente, os infográficos mais relevantes para o seu público (em empresas: 01, 02, 03 e 07; em escolas: 06; em bancos: 01, 02 e 05).
- **Antes da oficina:** percorra a apresentação uma vez lendo as notas do apresentador (modo "Apresentador" do PowerPoint). Cada nota indica o objetivo do slide e como trabalhá-lo.
- **Regra de ouro do facilitador:** a oficina alterna medo e solução. Nunca termine um bloco na ameaça: cada seção fecha com ações concretas — respeite essa ordem.

04 Agenda sugerida (50 minutos)

TEMPO	SLIDES	BLOCO	CHAVE DE FACILITAÇÃO
0–7 min	1–7	**Abertura.** O valor da sua vida digital, hackers vs. criminosos, o mapa das 5 portas.	No slide 2, peça que peguem o celular e olhem para ele: o exercício físico engaja. O 7 é o mapa: anuncie como promessa ("no final vocês vão saber fechar as cinco").
7–15 min	8–11	**Porta 1: golpes.** O e-mail armadilha, o teste faceb00k, como manipulam, o protocolo.	No 9, pergunte em voz alta qual endereço é o falso e espere respostas antes de revelar. A pausa seguinte é o momento mais importante da oficina.
15–21 min	12–14	**Porta 2: senhas.** O efeito dominó e a escada até as passkeys.	A pergunta do 12 ("você usa a mesma senha?") é retórica: não peça mãos levantadas, o humor do slide faz o trabalho.
21–28 min	15–18	**Porta 3: o celular.** O roubo minuto a minuto, os 4 cadeados, USB e QR.	A linha do tempo do 16 se lê devagar, marca por marca. O 17 é acionável: sugira configurar o PIN do chip (SIM) nessa mesma tarde.
28–34 min	19–21	**Porta 4: a casa.** Roteador, IoT e a regra dos dois lugares.	"A câmera que observa você" (20) costuma gerar perguntas: as respostas estão na seção 6 deste guia.
34–41 min	22–24	**Porta 5: a família.** Aliciamento, sexting, acompanhar em vez de proibir.	Abaixe a voz no 22 e não apresse o 23: é o pico emocional. Passe rápido ao 24 — nunca deixe os pais no medo sem ferramentas.
41–46 min	25–28	**Plano B + IA.** O que fazer se já aconteceu, o erro ilegal, deepfakes.	O 26 surpreende (contratar um "hacker" é crime próprio): deixe-o respirar.
46–50 min	29–30	**Encerramento + atividade.** O mapa completo, "uma porta hoje", folha de atividades.	Distribua a folha de atividades e encerre com a Atividade 3 (o compromisso escrito): pedir uma única ação multiplica a execução.

VERSÃO CURTA (25 MINUTOS)

Use os slides 1–2, 7–11, 12–14, 22–24 e 29–30 (abertura, golpes, senhas, família e encerramento). São as seções de maior impacto por minuto para públicos gerais.

05 As três atividades da folha

Atividade 1 — "Cace os sinais" (5 min, durante ou depois da Porta 1)

Cada participante marca com caneta os sinais de golpe em um e-mail impresso na folha. São **cinco**: (1) o domínio do remetente não é o oficial ("seubanco-avisos.net"), (2) a urgência de 24 horas, (3) o pedido de usuário e senha, (4) o link encurtado e (5) o prêmio inesperado no final. Corrija em voz alta: cada sinal encontrado em grupo vale mais do que dez explicados.

Atividade 2 — "Meus 10 cadeados" (3 min, perto do encerramento)

Checklist pessoal de hábitos. Não se entrega nem se compartilha: é um espelho individual. Sugira que cada um conte suas caixinhas vazias — esse número é a sua lista de tarefas da semana.

Atividade 3 — "Minha primeira porta" (2 min, encerramento da oficina)

Cada participante escreve **uma única ação** e **quando** vai fazê-la ("hoje à noite ativo o PIN do chip"). A evidência sobre intenções de implementação é clara: escrever o quando dobra a probabilidade de execução. Encerre a oficina lendo duas ou três em voz alta, com permissão.

06 Adaptações por público

PÚBLICO	AJUSTES RECOMENDADOS
Empresas	Enfatize as Portas 1 a 3 e o Plano B. Conecte com as políticas internas (relato de incidentes, MFA corporativo). Entregue os infográficos 01, 02, 03 e 07.
Escolas (para pais)	Dobre o tempo da Porta 5 (slides 22–24) e distribua o infográfico 06. Para aulas COM ALUNOS, não use esta apresentação: o kit inclui duas versões escolares dedicadas ("Guardiões da Internet" 8–12 e "Modo Defesa" 12–15), cada uma com seu próprio guia do professor e folha de atividades.
Bancos (para clientes)	Enfatize as Portas 1 e 2 mais o infográfico 05 (roubo de identidade e dinheiro). Reforce a mensagem "o banco nunca pede senhas por mensagem" com os seus canais oficiais.
Idosos	Versão curta (25 min), em ritmo mais calmo. Insista em duas regras: nada de dados por mensagem, e verificar ligando para um familiar de confiança diante de qualquer pedido de dinheiro.

07 Perguntas frequentes do público (e como respondê-las)

"OS GERENCIADORES DE SENHAS SÃO SEGUROS? E SE HACKEAREM O GERENCIADOR?"

Nenhum sistema é infalível, mas o gerenciador com uma senha mestra forte e MFA é muito superior à alternativa real: senhas repetidas ou anotadas. A comparação correta não é com a perfeição, e sim com o que a pessoa faz hoje.

"EU NÃO TENHO NADA A ESCONDER / NINGUÉM VAI ME ATACAR."

Os ataques atuais são massivos e automáticos: não escolhem vítimas, varrem. E todos temos algo a perder: o dinheiro da conta, a identidade (com a qual podem endividar você ou cometer crimes em seu nome) e o acesso a fotos e conversas suas e de terceiros.

"QUAL ANTIVÍRUS / GERENCIADOR / MARCA VOCÊ RECOMENDA?"

A oficina recomenda categorias e hábitos, não marcas: lojas oficiais, avaliações, quantidade de downloads e permissões razoáveis são os critérios para escolher qualquer produto. Evite recomendar marcas específicas, salvo política institucional própria.

"ACONTECEU ALGO PARECIDO COMIGO, O QUE FAÇO COM O MEU CASO?"

Não analise casos pessoais em público. Indique o protocolo geral (evidências, boletim de ocorrência na polícia, troca de senhas, canais oficiais) e encaminhe para uma conversa privada ou para um especialista.

"A IA NÃO TORNA TUDO ISSO INÚTIL?"

Ao contrário: a IA torna os golpes mais convincentes, mas as defesas da oficina não dependem de detectar erros de escrita, e sim de hábitos estruturais — verificar por outro canal, não entregar dados por mensagem, MFA. Esses sobrevivem aos deepfakes.

08 Checklist do facilitador

- [ ] Percorri a apresentação completa lendo as notas do apresentador.
- [ ] Imprimi uma folha de atividades por participante (e os infográficos escolhidos).
- [ ] Testei o projetor e o modo apresentador.
- [ ] Tenho à mão os links da academia, do simulador e do teste para compartilhar no encerramento.
- [ ] Sei qual é a minha versão (completa 50 min / curta 25 min) e a minha adaptação de público.

Este kit pode ser reproduzido e distribuído sem modificações para fins educacionais, citando o livro *Guia de Segurança de um Hacker*, de César Cerrudo — guiadeunhacker.com/pt/