SENSIBILIZAÇÃO

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção
Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação

Impressão
Divisão de Serviços Gráficos

SENSIBILIZAÇÃO

2021

CONTEÚDO

PNPC | PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

GUIA DE PROTEÇÃO DE CONHECIMENTOS SENSÍVEIS

Esta cartilha foi elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), desenvolvido pela Agência Brasileira de Inteligência (ABIN).

Criado em 1997, o PNPC é uma assessoria de segurança que busca promover cultura de proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas, com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

PNPC
PROTEGER COM INTELIGÊNCIA

1

ENGENHARIA SOCIAL

ENGENHARIA SOCIAL

Instituições nacionais são alvo constante de ações de engenharia social, método usado para enganar, manipular ou explorar a confiança das pessoas em busca de acesso a informações sensíveis e não disponíveis.

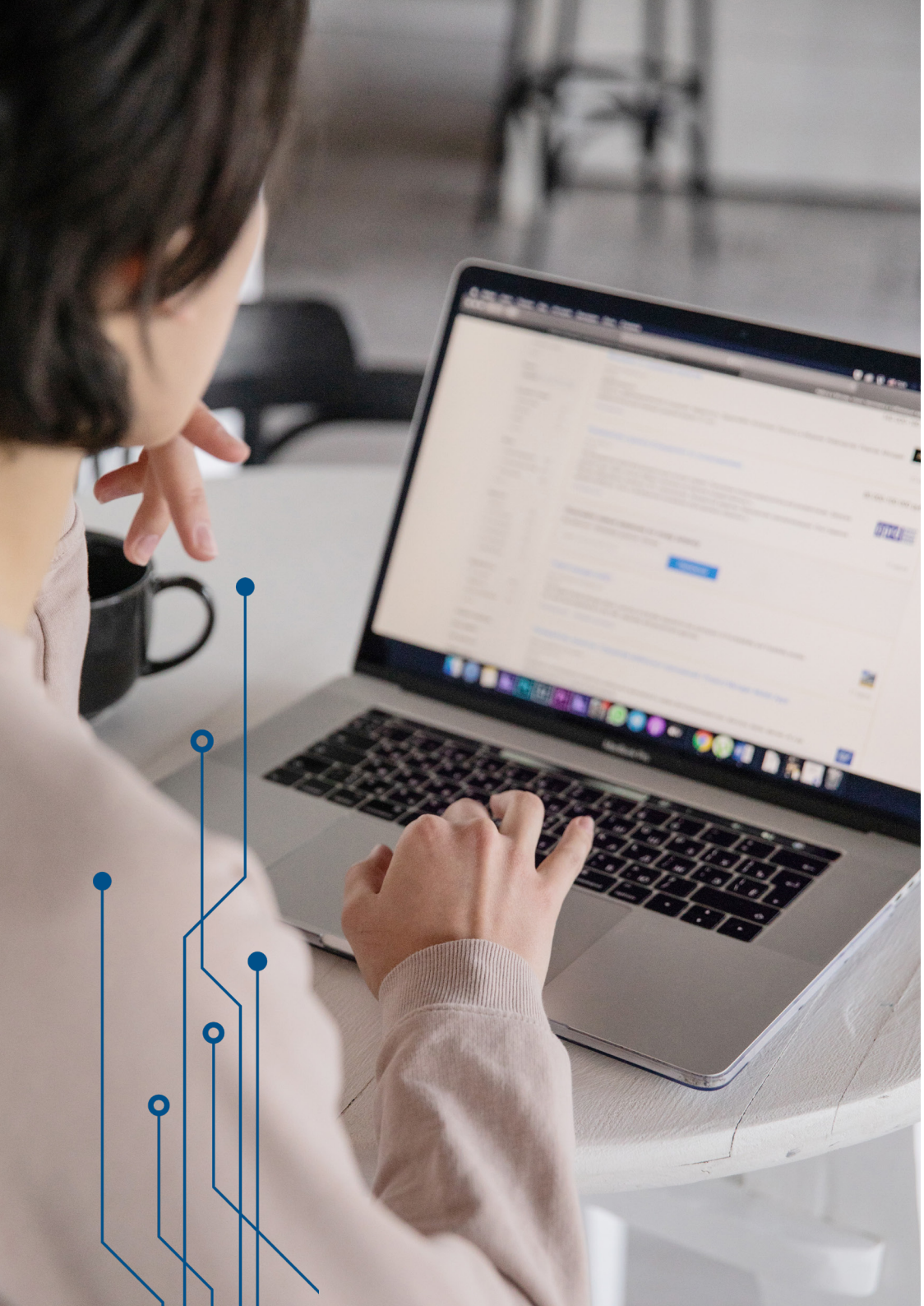
É uma forma de ataque sem violência física que busca fazer com que a vítima realize voluntariamente ações prejudiciais a si mesma ou a sua instituição.

A engenharia social pode ser utilizada por qualquer pessoa que tenha interesse em suas informações, desde serviços de Inteligência de Estados nacionais até hackers amadores.

PNPC
PROTEGER COM INTELIGÊNCIA

2

SEGURANÇA NA INTERNET



SEGURANÇA NA INTERNET

No trabalho

- Se você representa sua instituição on-line, pense cuidadosamente sobre o que você publica, limitando informações sensíveis sobre projetos e funcionários.
- Não presuma que as informações que você compartilha não irão além do destinatário original.
- Resista a ofertas tentadoras. Elas podem ser armadilhas para obtenção de informações sobre você.
- Não abra mensagens sem identificação ou se houver suspeita de endereço falso.
- Não use seu e-mail profissional para cadastramento em sites.
- Não acesse e-mails de anúncios (spam).
- Use cópia oculta para enviar mensagens a vários usuários.

PNPC
PROTEGER COM INTELIGÊNCIA

3
PROTEÇÃO NO CELULAR

PROTEÇÃO NO CELULAR

Aplicativos

- Instale um programa antimalware antes de baixar qualquer aplicativo.
- Baixe apenas aplicativos de lojas oficiais (app stores).
- Evite instalar aplicativos usando contas de redes sociais para não formar vínculos entre programas e bases de dados distintos.
- Instale versões mais recentes dos aplicativos assim que estiverem disponíveis.
- Verifique se as permissões solicitadas pelo aplicativo estão de acordo com suas funções e propósitos.
- Restrinja os acessos do aplicativo (localização, fotos, contatos etc.).
- Proteja informações pessoais - não comunique desnecessariamente nome, endereço, telefone etc.
- Desinstale aplicativos que você não usa mais.

Em **aplicativos de mensageria**, como WhatsApp, Telegram e Signal, ative a confirmação em duas etapas, em “configurações”.

Aparelho

- Evite usar wi-fi de ambientes públicos.
- Desligue wi-fi, bluetooth e localização quando não estiverem em uso.
- Na tela, desative notificações e habilite o bloqueio automático.
- Mantenha o sistema operacional atualizado com a última versão recomendada pelo fabricante.
- Habilite mecanismos de segurança, tais como criptografia da memória de armazenamento e fator duplo de autenticação.
- Não abra links de SMS não solicitados por você ou de remetentes desconhecidos.
- Ao se desfazer do seu smartphone, apague todos os dados e restaure as opções de fábrica.

PNPC
PROTEGER COM INTELIGÊNCIA

4

VIAGENS AO EXTERIOR

VIAGENS AO EXTERIOR

Antes

- Defina quais informações pessoais e profissionais podem ou não ser compartilhadas com entidades estrangeiras.
- Não leve materiais de trabalho com informações sensíveis que, se apreendidos, roubados ou extraviados, possam gerar riscos à instituição.
- Apague conteúdos sensíveis armazenados em seus aparelhos eletrônicos.
- Procure saber mais sobre o destino e os interlocutores estrangeiros.

Durante

- Evite conversar sobre assuntos sensíveis em locais públicos ou ao telefone, mesmo em português.
- Desligue o bluetooth e evite usar wi-fi e carregadores públicos.
- Não use aplicativos de mensageria ou e-mail particular para enviar informações sensíveis.
- Seja discreto em ambiente de trabalho ou de lazer. Tenha cuidado com abordagens de estrangeiros e desinforme seu acesso a informações institucionais.

Depois

- Faça check-up dos aparelhos após a viagem, para verificar eventual instalação de vírus.

- Não utilize pen drives presenteados e não abra anexos de e-mails ou links enviados depois de eventos patrocinados por estrangeiros, pois podem estar infectados com vírus espiões.

PNPC
PROTEGER COM INTELIGÊNCIA

5
VISITA DE DELEGAÇÕES

Quando você for o anfitrião, lembre-se de estabelecer limites entre a cordialidade e a preservação da informação sensível. Isso vale tanto para visitas institucionais quanto para congressos, palestras, cursos, reuniões e outros eventos.

Desconfie e relate se:

- Houver inclusão ou troca de pessoa de última hora.
- Os participantes marcarem reunião sobre um assunto e insistirem em outras pautas durante a visita.
- Alguém perguntar a mesma coisa para várias pessoas.
- Houver uso de eletrônicos não autorizados.
- Alguém insistir em tirar fotos ou exagerar no número de imagens.
- Houver pedido de forma reiterada para visitar área fora do roteiro de visita.
- Ocorrer tentativa de levantar nomes de pessoas com acesso a informações.

PNPC
PROTEGER COM INTELIGÊNCIA

6 REUNIÕES SENSÍVEIS

Antes

- Convide para a reunião apenas pessoas que tenham necessidade de conhecer o assunto discutido.
- Defina a pauta para evitar a abordagem de outros temas sensíveis que nem todos os presentes devam conhecer.
- Escolha sala ou auditório em local reservado e, se possível, com isolamento acústico.
- Limite o uso de aparelhos eletrônicos aos estritamente necessários e que sejam seguros e de procedência conhecida.

Durante

- Relembre aos presentes o caráter sigiloso da reunião e as regras de segurança que nortearão o encontro.
- Peça confidencialidade e, se necessário, assinatura de Termo de Compromisso de Manutenção de Sigilo.
- Oriente que documentos sensíveis sejam devidamente protegidos nos intervalos.
- Solicite que os assuntos sigilosos não sejam discutidos fora da sala.

Depois

- Alerte sobre a necessidade de manter documentos com anotações sensíveis em local seguro após o encontro, e que sejam carregados dentro de pastas.

- Em caso de compartilhamento digital, peça que o envio ocorra de forma segura, com uso de criptografia.

- Peça que assuntos sensíveis não sejam tratados em mensagens de aplicativos, como o WhatsApp.

- Lembre aos participantes que não é permitido comentar as decisões tomadas com outras pessoas que não tenham necessidade de conhecer.

PNPC
PROTEGER COM INTELIGÊNCIA

7
REDES SOCIAIS

Política pessoal

- Defina uma política pessoal de uso das redes sociais, identificando os objetivos a serem atingidos (compartilhar momentos com familiares e amigos, projeto pessoal destinado a alcance de maior engajamento digital, perfil profissional etc.). Há uma relação direta entre exposição e riscos.

- Controle a quantidade de usuários que podem ver o perfil, bem como a quantidade e o tipo de informações postadas, para evitar impactos indesejados.

Configurações de privacidade e segurança

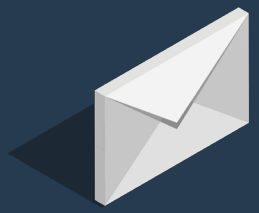
- Defina quem pode ver o quê e quais informações são públicas ou não.

- Ative o duplo fator de autenticação para que, em determinadas situações, seja necessária outra comprovação de sua identidade além da senha para acessar a rede.

Compartimentação de perfis

- Procure compartimentar seus perfis em redes sociais de forma que seja mais complicado o cruzamento de informações, usando nomes e apelidos diferentes, não estabelecendo links diretos entre as contas e usando diferentes fotos de capa.

- Se tiver um perfil público, estabeleça dois perfis dentro da mesma rede: um aberto e outro fechado, este para contato com amigos, familiares e publicação de assuntos mais pessoais sem que sejam vistos por todos.



Reporte

Caso acredite que sua instituição foi vítima de ação de espionagem ou sabotagem, avise sua chefia e o setor de segurança. Você também pode enviar um e-mail para **reporte@abin.gov.br** para estabelecer contato com a ABIN e relatar o caso.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR
WWW.GOV.BR/ABIN/PNPC