Centro Internet Segura

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Guia para campanha de sensibilização em 5 passos

Guia para campanha de sensibilização em 5 passos

A sensibilização para a ciber-higiene dos colaboradores é essencial para a resiliência de uma organização relativamente às ameaças no ciberespaço. Se tem a responsabilidade por essa matéria numa organização, encontra de seguida um guia em 5 passos que o ajuda a montar uma campanha de sensibilização junto dos colaboradores, de modo a reforçar a capacitação do fator humano na proteção contra incidentes de cibersegurança.

1

Estude as ameaças e o papel do risco humano para a cibersegurança na sua organização:

a. Identifique as principais ameaças para o ciberespaço que afetam o contexto nacional, o seu tipo de organização em particular e o setor onde esta atua (por frequência e impacto potencial das ameaças), considerando relatórios públicos sobre este tema e o histórico da organização;

b. Selecione, dessas ameaças, aquelas que mais utilizam as fragilidades do fator humano para concretizarem os seus fins;

c. Considere essas ameaças como as que devem merecer especial atenção na sua campanha de sensibilização.

Recursos:

- Relatórios *Riscos e Conflitos* do Observatório de Cibersegurança do CNCS;
- *Threat Landscape* da ENISA.

2

Caracterize o público-alvo, as mensagens a enviar e as metodologias a aplicar na campanha de sensibilização:

d. Defina o perfil do público-alvo na sua organização que deverá ser sensibilizado e segmente-o considerando as funções desempenhadas (ou outros aspetos de perfil sociodemográfico que considere relevantes, tais como sexo, idade e tipo/nível de formação);

e. Identifique as pessoas que mais lidam com informação sensível ou que estão mais expostas às ameaças, priorizando-as em relação às outras, se necessário;

f. Defina as mensagens que devem ser passadas a cada segmento do público-alvo considerando as principais ameaças que podem afetar o fator humano na sua organização e as funções desempenhadas pelos colaboradores em questão (em alguns casos, pode ser mais positivo não segmentar a mensagem, nomeadamente quando a organização é pequena ou as funções dos colaboradores são muito semelhantes) – uma mensagem é mais eficaz se for centrada nas ações a realizar, em forma de tutorial, do que se for baseada apenas no instigar do medo;

g. Escolha os canais mais adequados para cada caso (sessões presencias ou *online,* cursos *online,* conteúdos de boas práticas enviados por *email,* cartazes nas instalações, plataformas de gamificação, simulações de *phishing,* etc.) – a diversidade de canais e a interatividade das ações podem ser vantajosas porque permitem uma comunicação mais completa e com envolvimento;

h. Planifique a melhor forma de fazer chegar as mensagens aos colaboradores através dos canais e tipologias de conteúdos escolhidos, considerando um período temporal específico e os objetivos desejados.

Recursos:

- Relatórios *Sociedade* do Observatório de Cibersegurança do CNCS;
- Centro Internet Segura;
- Conteúdos para sessões presenciais ou *online* do CNCS;
- Conteúdos de boas práticas do CNCS;
- *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* (ENISA).

Realize as ações de sensibilização através dos canais escolhidos e no calendário previsto:

i. Promova as ações planeadas junto do público-alvo e facilite as inscrições caso estas se justifiquem;

j. Lance as mensagens de forma organizada, com sentido, destacando o que é mais importante e dirigindo-as a quem tem mais responsabilidades;

k. Paralelamente, mantenha os canais de comunicação ativos com o público-alvo de modo a realizar chamadas de atenção para ameaças do momento (por exemplo, alertas sobre campanhas de *phishing* que estejam a ocorrer).

Recursos:

- Cursos *online* do CNCS;
- Youtube do CNCS;
- Youtube do Centro Internet Segura;
- Alertas de cibersegurança do CNCS;
- Scamadviser;
- Krebs on Security;
- Schneier on Security.

Analise os resultados, mediante o estudo dos efeitos no público-alvo:

l. Defina um momento a partir do qual é razoável verificar a alteração de comportamentos depois de realizada uma campanha ou um período de envio de mensagens – é importante permitir que o público-alvo tenha tempo para assimilar e aplicar as boas práticas;

m. Analise os resultados nesse momento através de inquéritos, entrevistas, observação (se aplicável), simulações de *phishing* e/ou considerando os dados sobre incidentes recolhidos pela equipa responsável pela segurança informática na organização ou o SOC (Security Operations Centre), caso exista;
n. Avalie o grau de sucesso das ações empreendidas de forma crítica para que se realizem os ajustes necessários no próximo passo.

Recursos:

- Relatórios *Sociedade* do Observatório de Cibersegurança do CNCS;
- Inquéritos do Observatório de Cibersegurança do CNCS.

5

Atualize as ameaças, os conteúdos e as estratégias de sensibilização:

o. Periodicamente (por exemplo, anualmente), atualize os conteúdos e as estratégias com base nas ameaças mais importantes na atualidade – relativamente a ameaças emergentes resultantes de contextos inesperados, pode ser necessário desenvolver novos conteúdos e estratégias de resposta imediata;

p. Atualize também os conteúdos e as estratégias tendo em conta os resultados produzidos na etapa anterior (passo 4) – podem existir insuficiências na transmissão das mensagens que devem ser corrigidas;

q. Recomece o processo no primeiro passo, assumindo as atualizações e percorrendo os restantes passos de novo.

Recursos:

- Relatórios *Riscos e Conflitos* do Observatório de Cibersegurança do CNCS;
- *Threat Landscape* da ENISA.