HACK3R_
RANGERS

Erros mais comuns em programas de conscientização

É fácil encontrar conteúdos que tentam ensinar boas práticas na hora de criar um programa de conscientização em segurança da informação; o que é incomum é encontrar um material que lhe diga exatamente o que NÃO fazer para que eles deem certo.

Existe uma série de erros que são cometidos com frequência — seja por despreparo dos profissionais responsáveis pelo programa, por falta de investimento no assunto ou, simplesmente, por comodismo — que farão com que a eficácia do próprio seja drenada completamente.

O objetivo deste relatório é justamente apontar esses deslizes, de forma que você consiga evitá-los e, com isso, garanta uma taxa de engajamento maior por parte de seus colaboradores.

Com base nestas “dicas reversas”, ficarão ainda mais claros os pontos fracos de seu programa e a melhor forma de aprimorá-lo.

HACK3R_
RANGERS

1) Gastar muito tempo dos colaboradores de uma única vez: atividades de conscientização também não devem tomar muito tempo do participante: por isso, **evite vídeos muito longos** e cansativos, pois eles dificilmente serão aproveitados.

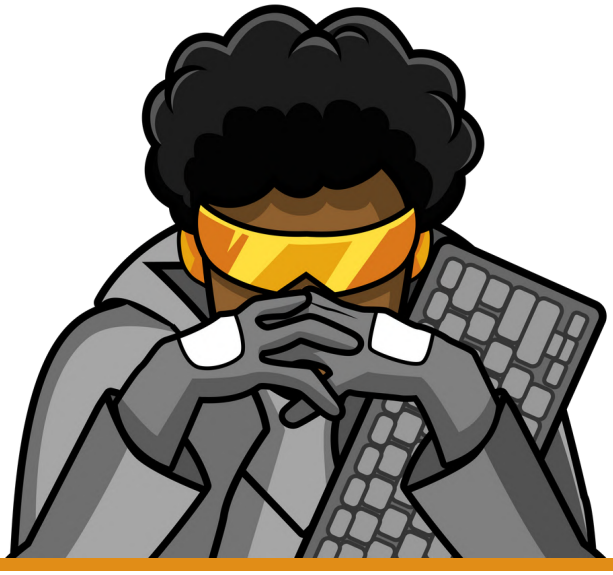
2) Reuso de materiais: um erro bastante comum é a prática de **reutilizar de forma constante** apresentações, cartilhas, quizzes e quaisquer outras ações educacionais. Tudo o que isso fará é reduzir o engajamento dos funcionários, que enjoarão rapidamente do programa.

3) Gastar muito tempo/dinheiro desenvolvendo seu próprio material: muitas empresas decidem internalizar ou contratar agências para criar os materiais de seu programa, **o que gera pouco volume de conteúdo (e sua inevitável reutilização)** e demanda um investimento financeiro mais alto do que contratar uma plataforma especializada em conscientização de cibersegurança.

4) Deixar de acompanhar métricas: evitou todos os erros até o momento? Parabéns! Agora, não se esqueça de evitar o próximo, que é justamente deixar de fazer um follow-up dos resultados de seu programa.

De nada adiantará se esforçar para criar um programa de qualidade se você não tiver métricas **para acompanhar o engajamento dos colaboradores (mudança de atitudes)** e a evolução de seu nível de conscientização.

Afinal, seu objetivo deve ser sempre subir no nível de maturidade SANS, causando mudanças culturais profundas nos hábitos de segurança de seu quadro de funcionários.



5) Não criar um programa contínuo: acredite ou não, mas há empresas que creem veementemente que realizar uma ação de conscientização anual é o suficiente para garantir que os seus colaboradores reconheçam ameaças cibernéticas. O crime digital evolui diariamente, o que exige um programa constantemente atualizado para refletir os riscos que os funcionários vão enfrentar em seu cotidiano.

E, se você fez a lição de casa e está testando o nível de conscientização dos participantes do programa com testes e simulações de phishing (por exemplo), tome cuidado com o próximo erro...

6) Envergonhar seus colaboradores: um programa de conscientização não deve apontar o dedo para quem está certo ou errado, mas sim ser inclusivo e incentivar a participação de todos. O erro faz parte do processo de aprendizagem e deve ser visto como natural.

7) Esquecer o porquê: pode parecer filosófico, mas não basta condicionar o comportamento seguro: ressalte, sempre que possível, a importância da segurança da informação e os perigos das ameaças cibernéticas (não apenas no âmbito corporativo, mas também na esfera pessoal). Dessa forma, o funcionário entende a importância daquele conhecimento em sua vida, de forma que os conteúdos didáticos serão fixados com maior facilidade.

HACK3R_
RANGERS

8) Não empoderar os colaboradores: da mesma forma que não devemos envergonhar os colaboradores, também não podemos nos esquecer de empoderá-los. Muitos gestores de SI enxergam o elo humano como simplesmente o mais fraco em sua estratégia de proteção de dados; a verdade, porém, é que uma equipe consciente pode ser a linha de frente contra ataques cibernéticos, reduzindo a forte dependência de softwares de cibersegurança.

9) Não envolver todos da empresa: até o momento, citamos o quadro de colaboradores como se a alta gerência não precisasse participar ativamente de seu programa de conscientização, sendo algo limitado a cargos operacionais. Este é justamente outro erro comum: acreditar que a conscientização é necessária apenas para funcionários plenos e sêniores. Gestores e diretores também precisam estar atualizados em relação aos perigos online!

Conscientizar usuários não precisa ser algo "chato" ou "apático".

10) Não seja "chato": no fim das contas, todos esses erros se resumem a um só: não seja apático. Não trate a conscientização em segurança da informação como um assunto chato ou uma obrigação, mas sim como parte da cultura corporativa. Programas podem sim ser divertidos e ter um alto nível de engajamento — especialmente com a gamificação da plataforma Hacker Rangers :)

Bibliografia
10 Security Awareness Training Mistakes to Avoid (Dark Reading, 10 de maio de 2021)

2021 Security Awareness Report (SANS, março de 2021)