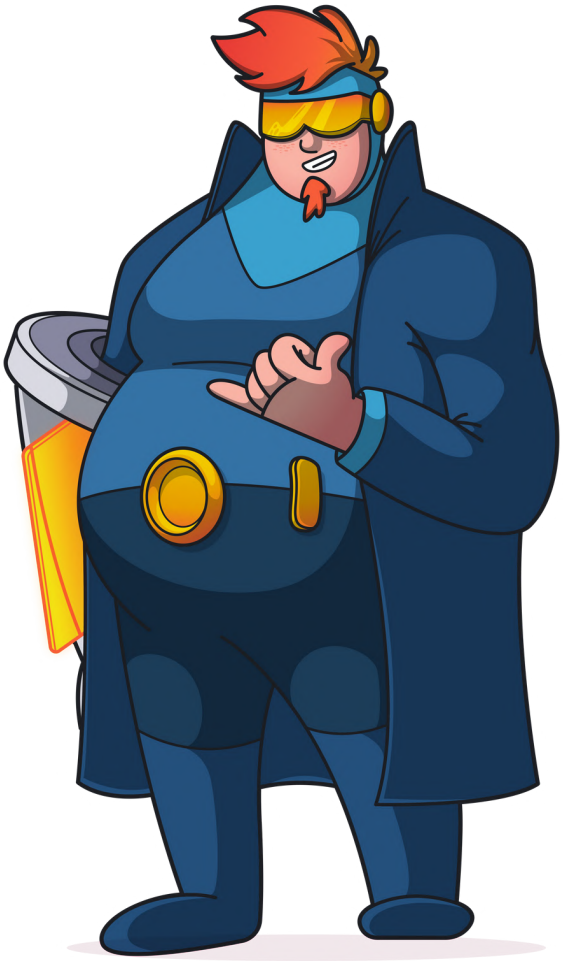
HACK3R_
RANGER5

CONSCIENTIZAÇÃO EM CIBERSEGURANÇA

Afinal, por que é tão importante?



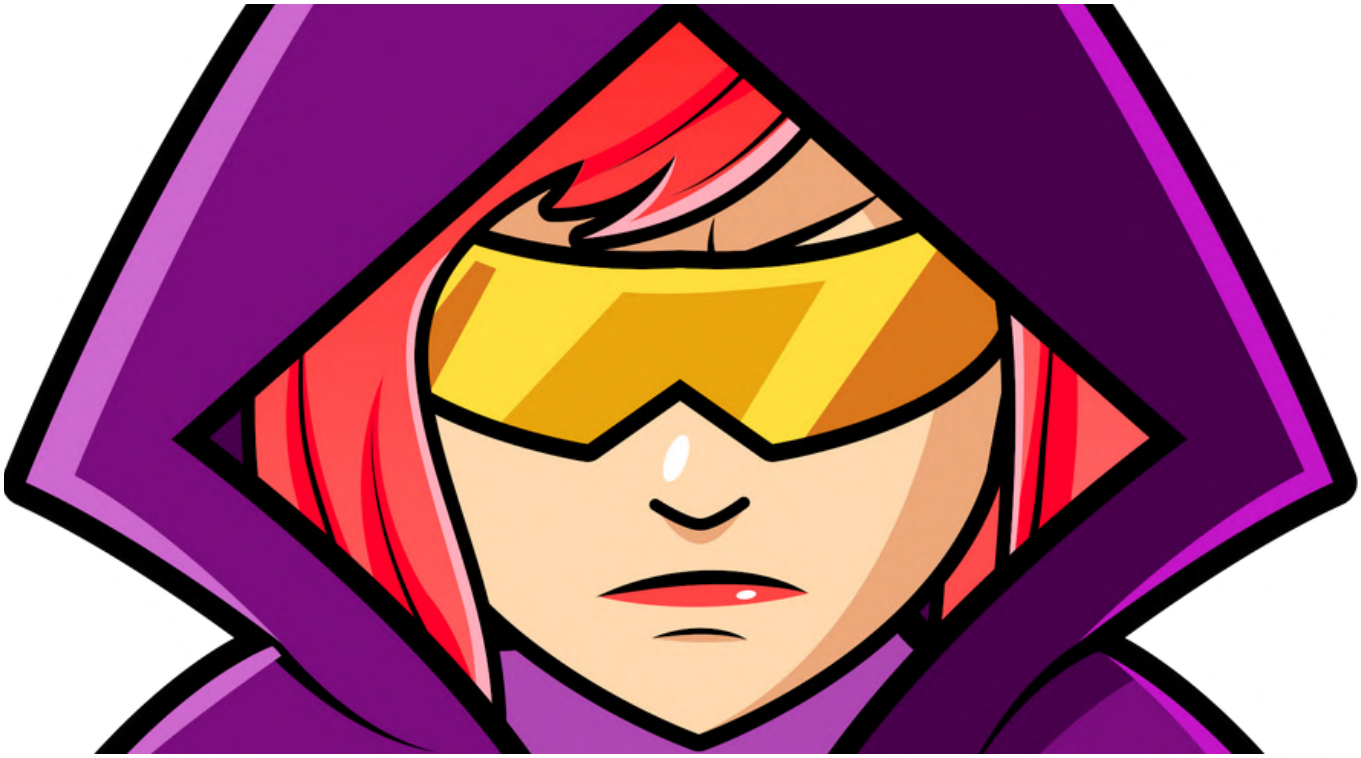
É como diz aquele velho ditado: há males que vêm para o bem. O aumento exponencial no número de crimes cibernéticos e incidentes de segurança da informação durante a crise do novo coronavírus (SARS-CoV2) finalmente despertou nas empresas o entendimento de que investir em medidas de segurança proativas podem salvá-las de prejuízos gigantescos.

Porém, vemos grandes investimentos em proteção de endpoint, em plataformas de acesso remoto seguro, em soluções de DLP... E o fator humano, infelizmente, continua menosprezado. Muitos gestores continuam acreditando que o software será o suficiente para garantir a proteção dos dados sensíveis de sua corporação.

Mas, afinal, por que é tão importante ter um programa de conscientização em cibersegurança? A resposta vai muito além da visão simplista que muitas pessoas possuem a respeito do tema. O objetivo deste relatório é demonstrar de forma didática e simples os benefícios de investir na conscientização dos seus colaboradores, respaldando tais fatos com estatísticas atualizadas do mercado.

MITIGANDO O ERRO HUMANO

Softwares de segurança, por si só, não garantem a segurança de seu ambiente corporativo. O ser humano presta um papel importante em qualquer estratégia de proteção de dados sensíveis.

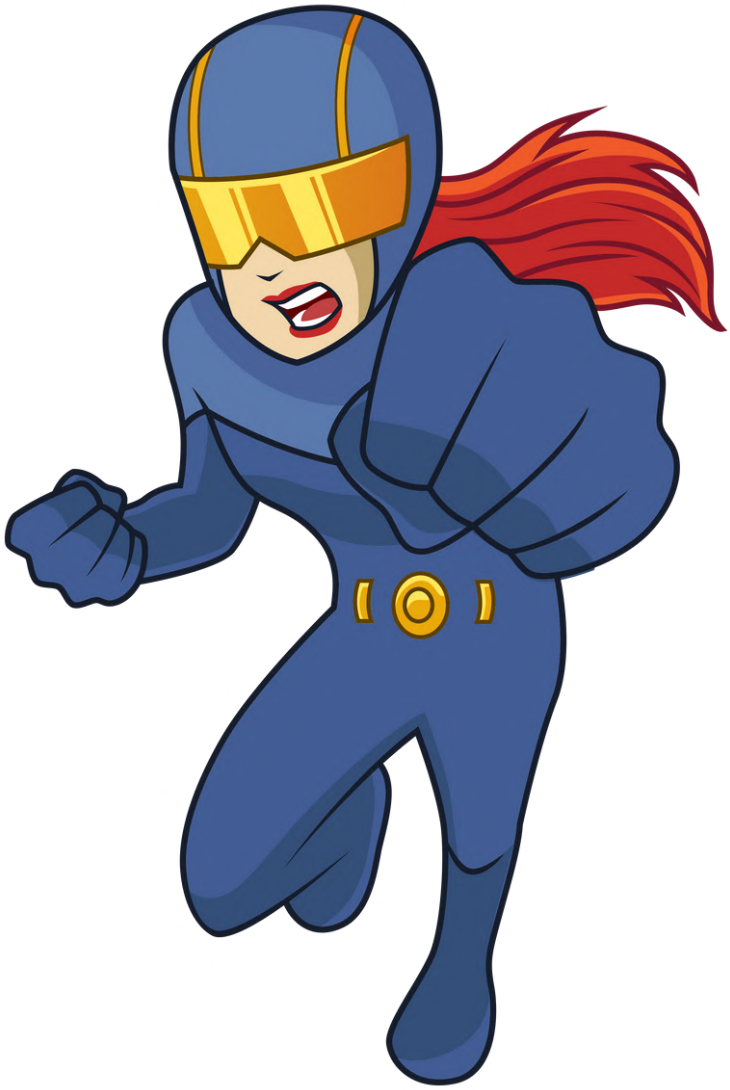


De acordo com um recente estudo publicado pelo Departamento de Cultura, Mídia e Esportes do Reino Unido, em 2019, erros humanos foram responsáveis por 90% dos incidentes de vazamentos de dados. Esse tipo de episódio costuma ser altamente danoso para as companhias: a mais recente versão da pesquisa anual da IBM, "The Cost of Data Breach", aponta que a exposição indevida de informações sensíveis custa, em média, US$ 3,86 milhões para uma empresa. Esse mesmo levantamento demonstrou que, a nível global, a negligência humana foi responsável por 23% dos casos; nos restantes, 62% foram ocasionados por credenciais roubadas, força bruta (o ato de invadir uma conta protegida por senhas fracas usando scripts automatizados) ou phishing.

E é neste ponto que você se pergunta: "onde estamos errando?". Historicamente falando, o ser humano é o elo mais sensível da cadeia de segurança da informação. Diferente de um software — que foi programado para agir de determinada forma e jamais fugir de seu escopo —, o ser humano pode ser facilmente manipulado usando aquilo que chamamos de engenharia social.

A engenharia social nada mais é do que a arte de se aproveitar dos sentimentos e dos vieses comportamentais de um indivíduo para convencê-lo (às vezes até sem querer) de fazer algo que ele geralmente não faria. E esse "algo", no mundo do cibercrime, sempre será algo que beneficiará o engenheiro social, como ceder uma senha ou abrir um malware.

Além disso, todos nós sabemos que conhecimento é poder. Inversamente falando, a falta de conhecimento leva o indivíduo a desconhecer as ameaças que o rondam, e, na internet, basta um passo em falso para cair em uma armadilha. Munidos de conhecimento, seus colaboradores deixam de ser alvos fáceis para os criminosos cibernéticos e se transformam em um verdadeiro exército de guerreiros que sabem desbravar os perigos da web, identificar riscos e trabalhar em equipe para mitigá-los. O fator humano e o software de segurança não são rivais e muito menos se anulam; muito pelo contrário. Eles são complementares, servindo como diferentes camadas para impedir que atores maliciosos invadam sua rede ou que dados confidenciais sejam roubados.



COMPLIANCE E COMPETIÇÃO

Mais do que uma obrigação, proteger os dados pessoais de seus consumidores se transformou em um verdadeiro diferencial competitivo. Programas de conscientização garantem uma cultura que valoriza a privacidade.

Na Europa, temos a General Data Protection Regulation (GPDR). No Brasil, temos a Lei Geral de Proteção de Dados (LGPD). O estado da Califórnia, nos EUA, possui seu próprio regulamento que visa proteger a privacidade dos cidadãos no ambiente digital; e há discussões em andamento para que o país crie uma norma a nível federal. Há dezenas de legislações ao redor do mundo com o mesmo propósito e, adivinhe? Praticamente todas elas exigem ou orientam as empresas a manterem um programa de conscientização em segurança cibernética. Aliás, a existência desse programa é um requisito obrigatório de compliance para determinadas áreas comerciais, incluindo o setor financeiro e o de pagamentos, que trabalham com padronizações bastante rígidas.

E, venhamos e convenhamos, mesmo que tais legislações não existissem, demonstrar cuidado com os dados pessoais de seu consumidor é algo que se tornou um diferencial competitivo. Felizmente, o número de internautas conscientes a respeito de seus direitos de privacidade no mundo online só cresce a cada dia. Eles estão preocupados com quais dados você coleta e o que faz com eles, tal como os esforços empreendidos na sua proteção. Afinal, tal como o crime cibernético causa prejuízos cada vez maiores para as empresas, o mesmo ocorre com os usuários finais, que passaram a ser vítimas constantes de golpes e fraudes financeiras. De posse de um banco de dados vazado, qualquer estelionatário pode praticar falsidade ideológica e causar danos à vida alheia.

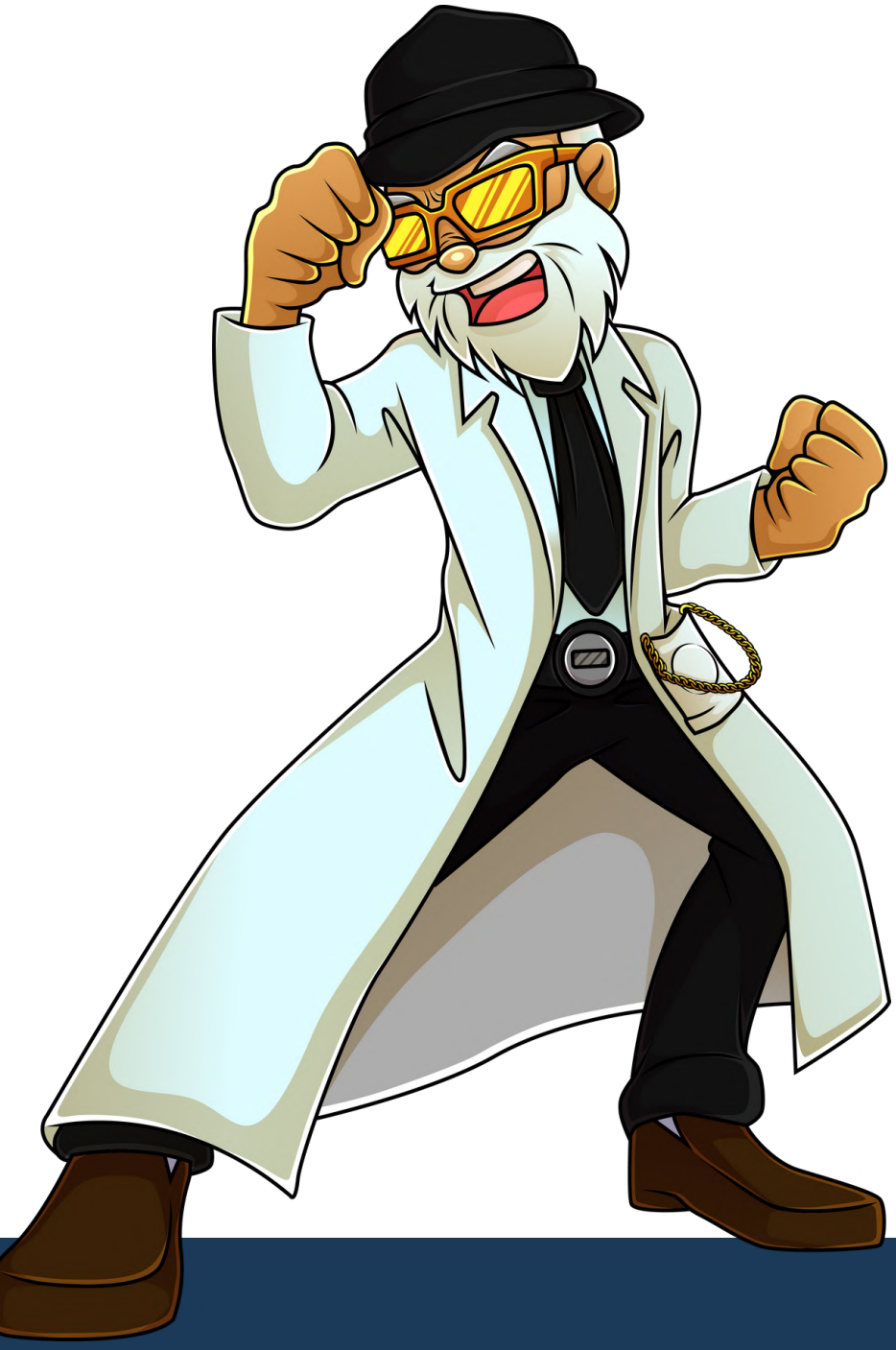
E o que a conscientização tem a ver com isso? Um programa de qualidade não se limita a condicionar o comportamento de seus colaboradores de forma robótica. Ele deve procurar, de fato, causar uma mudança cultural profunda, fazendo com que a preocupação com privacidade e proteção de dados se torne algo natural entre seus funcionários. É só dessa maneira que conseguimos garantir que todos os departamentos possíveis estejam perfeitamente alinhados com esse objetivo em comum; afinal, o marketing tem suas próprias necessidades, tal como o setor de recursos humanos, operações, vendas e assim por diante.

Não há forma mais eficaz de mostrar ao seu cliente que a sua marca respeita a sua privacidade e se preocupa com a segurança de suas informações do que com um bom programa de conscientização em cibersegurança. Quando os próprios responsáveis pelo armazenamento e tratamento de dados conhece o seu valor, entende os riscos envolvidos naquele processo e se coloca no mesmo patamar do usuário final, você pode dormir em paz tendo a plena certeza de que possui uma equipe que adotará a mentalidade privacy-first, tomando cuidado antes de adotar qualquer comportamento inseguro.

No fim das contas, todos se protegem mais e se beneficiam de uma web mais ética, segura e responsável.

PARA O BEM-ESTAR DE TODOS!

No fim das contas, um programa de conscientização em cibersegurança traz benefícios para todo mundo: sua empresa, seus colaboradores e os usuários finais!



Como citamos anteriormente, um programa de conscientização de qualidade não deve se limitar a condicionar um comportamento robótico, mas sim causar mudanças culturais profundas em seus colaboradores. Dessa forma, além de garantir a proteção da informação corporativa dentro do ambiente de trabalho, seus funcionários também levarão esses conhecimentos para seu círculo pessoal, o que os auxiliará a se protegerem no âmbito familiar.

E engana-se quem pensa que conscientizar o fator humano precisa ser algo chato e burocrático. Com uma plataforma gamificada como a Hacker Rangers, seus funcionários aprendem a se defender de uma forma divertida, participando de quizzes e competindo entre si de maneira saudável. Eles podem adquirir conhecimento necessário para se esquivar de e-mails de phishing, usar senhas fortes, identificar golpes de engenharia social e utilizar a internet de forma mais responsável.

No fim das contas, é um investimento no qual todos saem ganhando; sua empresa, seus colaboradores e a internet como um todo!

HACK3R_
RANGER5

TESTE A NOSSA PLATAFORMA GRATUITAMENTE DURANTE 15 DIAS!
HACKERRANGERS.COM.BR

Bibliografia

7 reasons why security awareness training is important (CybSafe, 26 de janeiro de 2021)

What is cyber security awareness and why is it important? (IT Governance, 27 de maio de 2021)