# 5 ERROS HUMANOS EM SEGURANÇA CIBERNÉTICA

HACK3R_ RANGERS

Entenda como a psicologia explica as posturas inseguras mais comuns (e perigosas) de seus colaboradores.

É um fato indiscutível: o fator humano possui um peso gigantesco quando o assunto é segurança da informação e proteção de dados confidenciais. De acordo com uma pesquisa da IBM realizada em 2021, erros humanos são a causa de 95% dos incidentes de segurança. Não é à toa que muitos consideram os colaboradores como "o elo mais fraco" de qualquer estratégia de cibersegurança.

Sabemos, porém, que não é bem assim. Neste relatório, vamos entender como a psicologia explica os erros em segurança cibernética cometidos pelos usuários e, claro, como uma adequada conscientização dos colaboradores pode ajudar a mitigar muitos desses equívocos!

HACK3R_ RANGERS

# QUAIS SÃO OS TIPOS DE ERROS HUMANOS?

## ERROS BASEADOS EM HABILIDADES

Os erros baseados em habilidade são aqueles causados pela imprudência momentânea do usuário e estão intimamente ligados a fatores externos — como um ambiente bagunçado, falta de atenção, fadiga, pressão para entregar uma tarefa, entre outros. Curiosamente, esses erros ocorrem quando o colaborador está realizando uma atividade que lhe é familiar: ele conhece as melhores práticas para concluí-la de forma correta, mas, por um deslize pontual, acaba adotando uma postura insegura que põe em xeque toda a estratégia de segurança cibernética da empresa.

Podemos citar, como um exemplo cada vez mais comum, os usuários que caem em fraudes de comprometimento de e-mail corporativo (Business Email Compromise ou BEC). Nesse golpe, o criminoso se passa por um executivo de alto escalão e solicita para um analista júnior do departamento financeiro, por exemplo, uma transferência financeira urgente de alto valor. Essa é uma tarefa que o colaborador está acostumado a fazer, mas, na ânsia de responder à urgência da situação, ele acaba não prestando atenção nos pequenos detalhes que poderiam ter revelado a farsa.

O trabalho remoto tem aumentado bastante a incidência de erros baseados em habilidades.

## ERROS BASEADOS EM DECISÕES

Os erros baseados em decisões ocorrem quando o usuário toma uma atitude equivocada mesmo quando possui o tempo e a atenção necessários para evitá-la. Nesses casos, em geral, a falta de conhecimento ou informação sobre uma determinada situação leva o colaborador a adotar uma postura insegura — já que ele não tem noção de que clicar naquele link, baixar aquele anexo, abrir aquele documento ou ignorar aquele aviso de atualização de algum software ocasionará uma falha de segurança.

A falta de conhecimento também se torna um risco associado ao ambiente no qual o indivíduo se encontra. Quando trabalha em sua própria residência, no modelo home office, ele pode se esquecer de que visitantes maliciosos podem obter acesso a documentos sensíveis ou de que outros membros de sua família podem usar o computador corporativo de maneira inadequada (acessando sites perigosos ou baixando jogos de fontes não confiáveis, por exemplo).

Da mesma forma, no escritório, a simples falta do bloqueio de tela e as inocentes conversas de elevador podem levar à exposição de informações privilegiadas. Com a popularização do trabalho híbrido e dos coworkings, esses são riscos cada vez mais comuns.

# OS 5 ERROS MAIS COMUNS

### 1) SENHAS FRACAS OU ARMAZENADAS INCORRETAMENTE

Estudos comprovam que uma senha de 12 dígitos composta unicamente por números pode ser descoberta em apenas 25 segundos. O uso de uma senha fraca para fazer login em sistemas corporativos é um erro comum que pode servir como porta de entrada para cibercriminosos. A falta do uso de um gerenciador de senha também é uma atitude perigosa.

### 2) USO DE SOFTWARES DESATUALIZADOS OU INSEGUROS

Atualizar aplicações costuma ser encarada como uma atividade "chata" pelos usuários, mas são cruciais para evitar vulnerabilidades exploradas pelos criminosos digitais. Também é comum o uso do chamado "shadow IT", que consiste no uso de aplicações não homologadas pelo departamento de TI que nem sempre são de fato seguras.

### 3) ENVIO INCORRETO DE DADOS SENSÍVEIS

Acredite ou não, o envio incorreto de informações é algo que está se tornando cada vez mais comum. Por conta da pressão do trabalho e das desatenções do ambiente residencial no modelo home office, muitos colaboradores estão simplesmente errando o destinatário ao enviar um e-mail contendo, por exemplo, um relatório recheado de dados sensíveis.

### 4) ARMAZENAMENTO NEGLIGENTE DE DADOS

Este ponto está relacionado ao shadow IT. Muitos colaboradores, por conveniência, armazenam dados sensíveis corporativos em plataformas e dispositivos pessoais (como serviços de armazenamento na nuvem ou pendrives e HDs externos). Obviamente, esses ambientes não possuem o mesmo nível de segurança em comparação com os dispositivos e serviços oficiais da empresa.

### 5) SER ENGANADO POR MEIO DE ENGENHARIA SOCIAL

Por fim, a engenharia social (usada em golpes de phishing, tailgating e muitos outros) continua sendo um risco onipresente envolvido nos mais diversos tipos de brechas de segurança.

HACK3R_
RANGERS

# MITIGANDO OS ERROS COM PROGRAMAS DE CONSCIENTIZAÇÃO

Uma recente pesquisa realizada pela Tessian revela que esses erros estão se tornando cada vez mais comuns com as mudanças sofridas recentemente no mercado de trabalho. Mais pressionados, com tarefas acumuladas e em ambientes recheados de elementos que tiram a sua atenção, é considerado natural que os colaboradores comentam deslizes com maior frequência. Por isso, as empresas precisam adotar uma abordagem mais humanizada, entender o cenário no qual os colaboradores estão inseridos e auxiliar o máximo possível na construção de uma cultura de segurança mais presente na vida do usuário.

Os programas de conscientização em segurança cibernética têm um papel importantíssimo nisso. Os conteúdos precisam ser adaptados para um formato mais leve e fácil de digerir, de forma que essas pílulas de conhecimento sejam absorvidas naturalmente no cotidiano do colaborador. Um treinamento constante, que exija a leitura de documentos longos e palestras excessivamente técnicas, pode surtir o efeito contrário, sobrecarregando os usuários e desestimulando ainda mais a cultura de segurança.

É por isso que a plataforma Hacker Rangers aplica gamificação e conceitos de nanolearning para garantir um processo de aprendizagem mais divertido e com alto nível de engajamento entre os seus colaboradores! Em uma era em que todos estamos saturados pela rotina de trabalho frenética, é essencial que os usuários possam aprender cibersegurança de forma leve e mudar seus hábitos enquanto se divertem. Com o Hacker Rangers, os colaboradores participam de uma competição saudável e lúdica que os incentiva a adotar pequenas posturas em seu cotidiano para mitigar a incidência dos erros citados neste relatório!

TESTE A NOSSA PLATAFORMA GRATUITAMENTE DURANTE 15 DIAS!

**HACKERRANGERS.COM.BR**


**Bibliografia**

*The Role of Human Error in Successful Cyber Security Breaches* (Usecure, julho de 2021)

*Top 5 human errors that impact cyber security* (Phriendly Phishing, novembro de 2021)

*Psychology of Human Error Report* (Tessian, abril de 2022)


HACK3R_ RANGERS