ENTREVISTA

ENTREVISTADOR: **Antonio Andrade – APDADOS**
ENTREVISTADO: **Vinicius Perallis, Founder da HACKER RANGERS**
TEMA: **Proteção de dados, cibersegurança e como a gamificação pode impulsionar a conscientização dos colaboradores.**

Contextualizando:

No cenário atual, onde a digitalização avança rapidamente, a cibersegurança e a proteção de dados tornaram-se questões cruciais para as empresas de todos os tamanhos. Com a implementação de regulamentos rigorosos como a Lei Geral de Proteção de Dados (LGPD) no Brasil, garantir que os colaboradores estejam bem-informados e conscientes sobre práticas seguras de manejo de dados é essencial. No entanto, as abordagens tradicionais de treinamento muitas vezes não conseguem captar a atenção e o engajamento necessários para uma efetiva conscientização.

É aqui que entra a gamificação – uma metodologia que utiliza elementos de jogos para tornar o aprendizado mais dinâmico e envolvente. Vinicius Perallis, Founder da Hacker Rangers, é um pioneiro nessa área, combinando cibersegurança com técnicas de gamificação para criar treinamentos que não só informam, mas também motivam os colaboradores a adotarem boas práticas de segurança.

Nesta entrevista, Vinicius compartilha conosco sua visão sobre os desafios da conscientização em cibersegurança, os benefícios da gamificação e como sua empresa está ajudando organizações a protegerem melhor seus dados. Vamos explorar as experiências e insights de Vinicius para entender como podemos transformar a maneira como lidamos com a cibersegurança nas empresas.

Perguntas:

1. Você poderia nos contar um pouco sobre a Hacker Rangers e como surgiu a ideia de combinar cibersegurança com gamificação?

A ideia da Hacker Rangers sempre esteve comigo de alguma forma desde o início da minha carreira. Desde que me formei em Ciências da Computação pela UNESP de Rio Claro, sabia que queria trabalhar com cibersegurança. Trabalhei como DBA na IBM, Sicoob e no Ministério do Desenvolvimento Social por quatro anos.

Mas percebi rapidamente que o maior desafio da cibersegurança residia na camada humana. As pessoas eram a maior porta de entrada para brechas de segurança nas empresas, e o treinamento e a conscientização delas não estavam sendo realizados com o devido cuidado e de uma forma que realmente as envolvesse e as fizesse entender a importância do seu papel na segurança.

Foi então que, em 2011, decidi mudar minha vida e começar tudo do zero em Campinas, onde fundei a Perallis Security. Alguns anos depois, surgiu a Hacker Rangers, a primeira solução 100% gamificada do mundo para conscientização em cibersegurança.

Através da gamificação, conseguimos tornar o treinamento em cibersegurança mais envolvente e eficaz, trazendo as pessoas para mais perto do processo e aumentando a conscientização sobre a importância da segurança digital.

2. Quais são os maiores desafios que as empresas enfrentam hoje em relação à conscientização dos colaboradores sobre cibersegurança e proteção de dados?

Atualmente, me parece que o maior desafio que as empresas enfrentam hoje é a natureza passiva do aprendizado tradicional quando falamos em cibersegurança, além da pontualidade dos treinamentos.

É comum que os colaboradores sejam expostos a treinamentos que envolvem apenas assistir a vídeos ou palestras, sem interação ou envolvimento ativo, muitas vezes apenas uma ou duas vezes por ano.

Em uma rotina de trabalho corrida, é difícil captar e manter a atenção dos colaboradores, e ainda mais difícil fazer com que eles apliquem os conhecimentos adquiridos em suas atividades diárias.

Com métodos de treinamento passivos, esse desafio se torna ainda maior, porque eles dificilmente despertam o interesse dos membros da equipe, e não os incentiva a colocar o aprendizado em prática.

Para criar uma cultura de proteção de dados, precisamos de métodos de treinamento mais dinâmicos e envolventes, que incentivem a participação ativa e o engajamento contínuo dos funcionários na segurança cibernética.

3. Como a gamificação pode ajudar a superar esses desafios? Poderia nos dar alguns exemplos práticos de como isso funciona na Hacker Rangers?

A gamificação vem justamente para transformar o cenário dos treinamentos em cibersegurança, tornando-os mais dinâmicos e interessantes para os colaboradores.

A ideia de um treinamento gamificado é fazer dos colaboradores os protagonistas da jornada de cibersegurança da empresa. Isso é fundamental porque, no final das contas, a equipe é a última linha de defesa contra ataques cibernéticos, então todo o treinamento deve ser pensado com foco neles.

No Hacker Rangers, por exemplo, implementamos um sistema de rankings e patentes que motiva os colaboradores a se dedicarem ao programa. Eles competem para ficar entre os primeiros colocados, conquistando medalhas e outros reconhecimentos. Esses elementos de gamificação não só engajam os colaboradores, mas também criam um ambiente de aprendizado contínuo e ativo.

Uma medalha após completar uma mini missão pode parecer simples, mas desperta a motivação para continuar praticando, pois representa o reconhecimento de uma pequena vitória. E é reconhecendo e celebrando essas pequenas vitórias que nós conseguimos uma grande vitória: o sucesso da empresa ao implementar uma cultura proteção de dados.

4. Você acredita que a gamificação é mais eficaz do que os métodos tradicionais de treinamento em cibersegurança? Por quê?

Sem dúvidas. A gamificação coloca o colaborador no centro do processo de cibersegurança, tornando-o um participante ativo em vez de um mero espectador. Um treinamento gamificado tem como base o reconhecimento contínuo, em que o colaborador é recompensado pelas pequenas ações que coloca em prática no dia a dia.

Por exemplo, no Hacker Rangers, temos o canal de "Ciberatitudes". Por meio dele, os colaboradores podem informar qualquer atitude segura que tenham tomado e ganhar pontos por isso. Eles podem, por exemplo, informar que habilitaram a autenticação em dois fatores no celular após assistir a um curso

sobre o tema, ou reportar que encontraram um risco de segurança na empresa, como um documento importante em uma pasta pública.

Essas "Ciberatitudes" incentivam os colaboradores a permanecerem atentos no cotidiano e a informar a empresa sempre que uma situação suspeita for identificada. Isso cria uma cultura de vigilância contínua, onde todos na empresa, não apenas a equipe de cibersegurança, estão envolvidos na proteção dos dados. É como ter olhos em todos os lugares a todo momento.

Quando eles informam que tomaram atitudes seguras, ganham pontos por isso. E isso é recompensador para eles! Quando somos recompensados por alguma boa ação que tomamos, o cérebro libera dopamina e serotonina, os hormônios do bem-estar e da felicidade.

Isso associa o aprendizado com uma sensação positiva, incentivando os colaboradores a continuarem praticando ações semelhantes. É dessa forma que a gamificação torna o treinamento mais eficaz, saudável e engajador.

5. Poderia compartilhar conosco algum caso de sucesso onde a metodologia da Hacker Rangers fez a diferença na proteção de dados de uma empresa?

Claro. A Azul Linhas Aéreas é uma empresa que tem se destacado na conscientização em cibersegurança dos seus colaboradores. Eles são um exemplo perfeito de como a gamificação pode fazer diferença no dia a dia de uma empresa.

Em 2023, eles iniciaram uma jornada com a gente para a sua primeira temporada de treinamento gamificado. Com muita dedicação, seguiram todas as boas práticas recomendadas pelos especialistas da Hacker Rangers.

O resultado? Durante a temporada, a equipe de cybersecurity recebeu milhares de ciberatitudes. Mais de 600 delas resultaram em melhorias concretas para a área de cibersegurança.

Esse resultado demonstra, na prática, o impacto positivo da gamificação e da criação de uma cultura de proteção de dados. Quando você tem olhos em todos os lugares, há mais chances de identificar e corrigir brechas de segurança.

Cria-se, então, uma cultura de vigilância contínua, fortalecendo a segurança da empresa como um todo.

6. A LGPD trouxe novas responsabilidades para as empresas em termos de proteção de dados. Como você vê a relação entre a conformidade legal e a conscientização dos colaboradores?

A conscientização dos colaboradores é uma peça essencial no quebra-cabeça da proteção de dados, e isso não é exigido apenas pela LGPD, mas também por várias outras normas e regulamentações relacionadas à segurança da informação, como as normas ISO 27001 e 27002, a Circular Bacen 3909, e o PCI DSS.

Embora a conformidade legal exija a implementação de um programa de conscientização, a cultura de cibersegurança precisa ir além do simples cumprimento de requisitos legais para ser realmente eficaz.

É preciso que a segurança da informação seja incorporada à cultura da empresa. Para isso, o treinamento em cibersegurança precisa ser contínuo e regular.

Uma cultura de cibersegurança bem estabelecida envolve educar e engajar os colaboradores de maneira constante, garantindo que eles compreendam a importância da proteção de dados e estejam atualizados sobre as melhores práticas e ameaças emergentes.

Só assim é possível transformar a conformidade legal em uma prática eficaz e

integrada ao dia a dia da empresa, criando um ambiente onde todos participam ativamente na proteção dos dados e na prevenção de riscos.

7. Em um cenário onde as ameaças cibernéticas estão em constante evolução, como a Hacker Rangers mantém suas abordagens de gamificação atualizadas e relevantes?

A Hacker Rangers lança pelo menos quatro novos cursos e quizzes a cada mês para acompanhar as novas ameaças e tendências em cibersegurança. Também criamos e disponibilizamos novos desafios e enviamos notificações para nossos

clientes informando sobre a publicação desses conteúdos, para estimular ainda mais o interesse dos colaboradores.

Estamos sempre em busca de novas formas de inovar e incorporar ainda mais elementos de gamificação, não apenas para os colaboradores, mas também para os próprios gestores. Por exemplo, mensalmente, reconhecemos os clientes com os melhores programas de conscientização. Estamos comprometidos em tornar os treinamentos cada dia mais eficientes para todos.

8. Quais são as principais tendências que você vê emergindo no campo da cibersegurança e da proteção de dados nos próximos anos?

Acredito que, nos próximos anos, veremos a transição de um foco puramente em "treinamento em cibersegurança" para um enfoque mais amplo que chamamos de "gerenciamento do risco humano", como já está acontecendo nos Estados Unidos e na União Europeia, por exemplo, que têm mercados mais maduros nesse âmbito.

Com a evolução da inteligência artificial, as fronteiras entre o real e o falso estão se tornando cada vez mais indistinguíveis. Isso significa que, mais do que nunca, precisaremos de abordagens de conscientização que incentivem a proatividade e a capacidade de responder rapidamente a ameaças cibernéticos.

No lugar de se limitar a treinamentos pontuais ou ser encarados apenas como requisitos para cumprimento de normas, me parece que passaremos finalmente a entender a conscientização em cibersegurança como estratégia fundamental para mitigação do risco humano nas empresas.

Isso implica em criar programas de cibersegurança contínuos, que integrem todos os colaboradores no processo de proteção e promovam uma cultura de segurança que se perpetuará no dia a dia.

9. Que conselhos você daria para empresas que estão começando a implementar programas de conscientização sobre cibersegurança?

O principal conselho que eu daria é: mantenha o programa de conscientização em cibersegurança em continuidade. A conscientização em cibersegurança não deve ser vista como um projeto com um prazo final, mas sim como uma jornada

contínua. Assim como você não desliga seu antivírus ou outras ferramentas de segurança, você também não pode "desligar" o programa de conscientização. Um cibercriminoso precisa de apenas um único clique para colocar a segurança de uma empresa em xeque.

Por isso, é essencial educar e engajar os colaboradores de maneira constante. Somente dessa maneira é possível transformar as boas práticas de segurança em hábitos e realmente criar uma cultura de proteção de dados. Afinal, cultura é isso: é ter a segurança como "configuração padrão" nas atitudes de todos os colaboradores todos os dias.

Segundo a SANS, uma das maiores referências no mercado de segurança cibernética, um programa que é pontual ou puramente focado em compliance pode ser mais perigoso do que não ter um programa nenhum. Isso ocorre porque eles geram uma falsa sensação de segurança: a empresa se sente protegida quando, na verdade, pode estar vulnerável.

Portanto, foque em criar um programa que envolva e motive os colaboradores de maneira constante. Cuide de suas necessidades de aprendizado, adapte os treinamentos à realidade da sua empresa e conte com a gamificação para aumentar os níveis de engajamento.

10. Por fim, como você vê o futuro da gamificação no contexto da cibersegurança? Existe algum novo projeto ou inovação que a Hacker Rangers está desenvolvendo e que você possa compartilhar conosco?

A gamificação está mudando o jogo quando se trata de cibersegurança. Ela é uma ferramenta poderosa não apenas para engajar os colaboradores, mas também para oferecer novas formas de enfrentar velhos desafios, entendendo os problemas de segurança de outra perspectiva.

Atualmente, estamos muito empolgados com um novo projeto na Hacker Rangers: o PhishOS. É um jogo interativo em que os colaboradores ajudam um dos nossos personagens, os Rangers, a identificar se um e-mail é phishing ou não. A metodologia do PhishOS é inteiramente baseada na NIST Phishing Scale, uma referência técnica crucial que define uma série de critérios para identificar e-mails maliciosos.

O que eu mais gosto no PhishOS é que ele vai além das métricas tradicionais de simulações de phishing, que muitas vezes só avaliam se alguém clicou ou não

em um link. Essas simulações costumam fornecer poucos insights, pois não revelam se o colaborador realmente reconheceu o e-mail como malicioso ou se ele apenas optou por não clicar porque adotou uma postura defensiva com relação ao treinamento.

No PhishOS, o colaborador é estimulado a identificar todos os sinais que indicam que um e-mail é phishing. Caso algum indício seja perdido, ele recebe um alerta e tem a oportunidade de revisar o que foi deixado passar.

Isso permite que as empresas não apenas verifiquem se os colaboradores conseguem identificar e-mails de phishing, mas, mais importante, se eles compreendem e conseguem justificar os motivos pelos quais um e-mail é malicioso.

O PhishOS não só reforça o aprendizado de forma prática, mas também possibilita que o gestor veja exatamente como o colaborador está aplicando o conhecimento. É uma maneira mais eficaz de garantir que o treinamento realmente faça a diferença no dia a dia.