Programa de Conscientização em **Segurança da Informação**





Ficha Técnica

EMPRESA
CTG Brasil

PROJETO
Programa de Conscientização em Segurança da Informação

RESPONSÁVEIS PELO PROJETO
Salete da Hora
Diretora de Marca, Comunicação e Sustentabilidade – CTG Brasil
Responsável pela estratégia, comunicação e engajamento

Flaviano Souza
Diretor de TI
Responsável pela coordenação técnica e engajamento

Gilson Henrique Silva
Analista de Segurança da Informação
Responsável pela criação, arquitetura, criação de conteúdo, manutenção e monitoramento do programa.

Mariana Olívio
Analista de Comunicação
Responsável pela produção de conteúdo e divulgação interna

Leticia Pfitzenmeier
Estagiária de TI
Responsável pela criação de conteúdo, manutenção e monitoramento do programa

Rodrigo Araújo
Estagiário de Comunicação
Suporte operacional e de produção de conteúdo

CTG Brasil

Índice

Resumo 5

Contexto 6

Estratégia e Ações 7

Despertando o Interesse 7

Cronograma 8

Programa de Conscientização em Segurança da Informação 8

Engenharia Social 14

Segunda Fase 15

Com a palavra, os jogadores 18

Investimentos 19

Resultados 19





Resumo

Às vésperas da pandemia, a CTG Brasil lançou um programa inovador de segurança da informação. A organização trocou os esporádicos informes técnicos sobre cuidados que deveriam ser tomados no dia a dia com a segurança da informação pessoal e da companhia por um programa lúdico baseado em gamificação, desafios, web séries e mudança de hábitos que valiam prêmios.

Com desafios semanais que premiam mudanças de atitude como habilitar dupla autenticação no celular ou trocar as senhas periodicamente, a campanha de divulgação do programa é conduzida por dois personagens que conhecem todas as armadilhas virtuais e que ajudam os profissionais da CTG Brasil a não cair em nenhuma delas. A atualização do conteúdo é semanal oferecendo tutoriais, dicas, exemplos de situações e mostra os mais novos "golpes virtuais" encontrados na web. Além da plataforma que mistura informação e entretenimento, a própria CTG Brasil simula armadilhas no dia a dia, como e-mails phishing e spam, para verificar quem está atento ao tema.

Produzido majoritariamente com recursos internos e com participação voluntária dos funcionários, o programa conseguiu engajar mais da metade da comunidade CTG Brasil logo no seu lançamento. Em seu segundo ano, agregou novos recursos e, além da premiação individual, passou a oferecer certificado de reconhecimento para as melhores performances por área da empresa, pelo engajamento coletivo, incentivando assim o trabalho em equipe.

Com a transferência de toda a parte administrativa para o sistema *home office* em virtude da pandemia da Covid-19, o Programa de Conscientização em Segurança da Informação se transformou também em uma maneira de deixar os profissionais mais próximos e com mais interação durante a pandemia.

Contexto

Segurança digital é um tema cada vez mais sensível em empresas de todos os portes. Uma área que vem exigindo investimentos constantes, rapidez na detecção e resolução de problemas e a presença de um capital humano que consiga antever situações e agir imediatamente. Se por um lado as organizações investem quantias vultuosas em sistemas de segurança e treinamentos, por outro as armadilhas são cada vez mais tentadoras, rápidas e difíceis de detectar, pois parecem mensagens reais. Anos de investimento na construção de sistemas de segurança da informação com vigilância e aprimoramento diários podem ir por água abaixo com um único clique dado remotamente em um *link* enviado por e-mail ou mensagem, ou ainda pela conexão de um *pen drive*. Em alguns segundos, milhões podem ser perdidos com o sequestro de senhas, dados e informações, os chamados ataques de *ransomwares*. A empresa pode literalmente parar se não pagar quantias vultuosas aos sequestradores digitais para ter seu sistema de volta.

Em 2019, o Brasil era o terceiro país no mundo que mais sofria ataques cibernéticos, ficando atrás apenas dos Estados Unidos e da China, conforme divulgado em um levantamento da Symantec, uma das principais organizações mundiais voltadas para a segurança da informação. Quando o assunto é sequestro de dados, o Brasil vai para a vice-liderança de acordo com o *Fast Facts*, relatório anual da *Trend Micro*, outra empresa global de segurança da informação. Perde apenas para os EUA. Com a pandemia, esse cenário se tornou ainda mais arriscado, pois uma grande quantidade de profissionais foi trabalhar em sistema *home office*, uma prática que deve permanecer no longo prazo, ao menos parcialmente.

Um levantamento feito pela *Fortinet Threat Intelligence Insider*, outra plataforma mundial voltada para a segurança da informação, mostrou que entre os meses de janeiro e setembro de 2020, houve mais de 3,4 bilhões de tentativas de ataques via internet no cenário internacional.

Dificilmente um hacker entra em um sistema organizacional se ninguém abrir a porta, mesmo que não saiba que está abrindo. E retirar a ou minimizar o acesso da empresa à rede mundial de computadores é algo fora de questão. As organizações operam cada vez mais em nuvem e, em locais remotos, atuam às vezes até sem a presença humana. É preciso proteger o patrimônio virtual. E o conhecimento é uma forte arma nessa guerra.

QUEM É A CTG BRASIL

Em atividade no Brasil desde 2013, a CTG Brasil é uma empresa do grupo China Three Gorges Corporation, o mesmo responsável pela construção e operação da maior usina hidrelétrica do mundo: a Três Gargantas, na China. A empresa, que nasceu naquele país com o intuito de controlar cheias do Rio Yangtzé, promover o turismo regional e gerar energia, se tornou uma das líderes mundiais em geração de energia limpa. No Brasil, é a segunda maior geradora privada de energia, com investimentos em 17 usinas hidrelétricas e 11 parques eólicos, estando presente em mais de 10 estados, com capacidade instalada de 8,3 GW.

Estratégia e Ações

A CTG Brasil sempre teve grande preocupação com o tema, destinando esforços e recursos para manter sistemas de ponta para proteger seus dados corporativos de ataques virtuais. Periodicamente, mas sem frequência definida, a empresa enviava informações e promovia palestras sobre segurança digital. Apesar dos esforços em informar a equipe, o engajamento nos procedimentos de segurança digital por parte dos colaboradores não atingia as expectativas.

Um dos principais motivos para essa falta de engajamento era a maneira como a informação era transmitida. As campanhas de segurança da informação eram muito técnicas, trazendo proibições e às vezes com tom punitivo. Campanhas proibitivas e sem atrativos comunicacionais dificilmente sensibilizavam alguém além da própria área de TI.

Até que, no final de 2019 e início de 2020, a empresa decidiu que precisava mudar esse jogo. A CTG Brasil resolveu que o tema poderia ser tratado de maneira divertida e com viés positivo, mas sem perder o foco na gravidade e importância do problema.

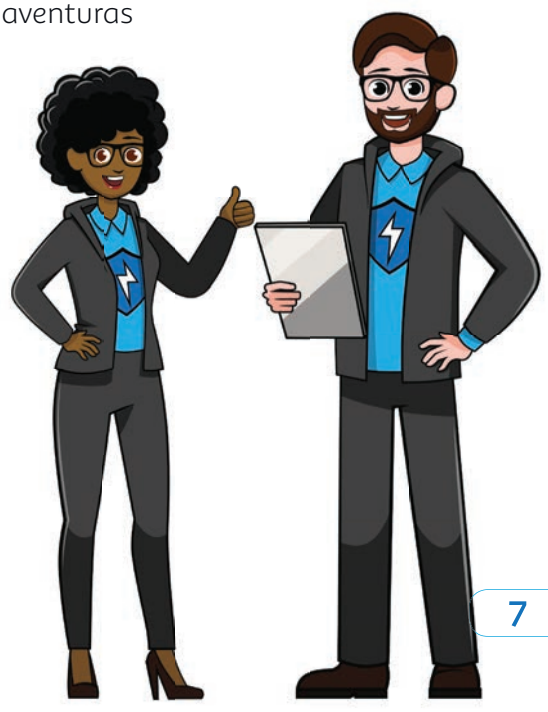
O primeiro passo foi engajar a liderança, que aceitou a ideia com facilidade. O vice-presidente e os diretores de TI e Comunicação se engajaram pessoalmente em propagar a ideia. A etapa seguinte era estruturar o processo de maneira atrativa para todos os públicos da empresa.

Surgiu então o **Programa de Conscientização em Segurança da Informação**. Aplicado na plataforma *Hacker Rangers*, ele foi lançado em março de 2020, algumas semanas antes do anúncio da pandemia, quando todo o setor administrativo passou a trabalhar de maneira remota. O programa contava com uma campanha elaborada em três fases, utilizando-se das novas mídias e de um sistema gamificado em uma plataforma interativa, recheada de conteúdos lúdicos e divertidos. Dessa maneira, uma ação que até então era percebida como cerceadora se transformou em um processo de aprendizagem colaborativo e motivador e, principalmente, muito divertido.

DESPERTANDO O INTERESSE

Inicialmente, a CTG Brasil direcionou sua comunicação para despertar a curiosidade da equipe. Uma campanha com memes e teasers inundou as caixas de e-mail dos colaboradores. Sem nenhum anúncio oficial do programa, os profissionais começaram a receber e-mails avisando que algo novo estava para acontecer e que a empresa estaria contando com a participação de cada um. As informações foram reveladas aos poucos. Todas as peças foram concebidas em português e em inglês, com o intuito de atingir também os expatriados que vivem no Brasil e funcionários de outros países que, porventura, estariam temporariamente realizando alguma atividade por aqui.
O programa foi aberto a terceiros que prestam serviços constantes para a empresa.

Ainda na fase de lançamento foram criados dois personagens representando a diversidade dos profissionais. Esses personagens eram os porta-vozes da proposta e conduziriam as aventuras que seriam vividas por todos em busca de sua segurança da informação.



Cronograma

DATA	ETAPA
novembro/2019 a fevereiro/2020	Concepção do projeto e divulgação de teasers.
março a dezembro/2020	Lançamento da plataforma e primeira, segunda e terceira temporadas da campanha de 2020.
janeiro a dezembro/2021	Primeira, segunda – e terceira temporadas – em andamento ao longo de 2021.

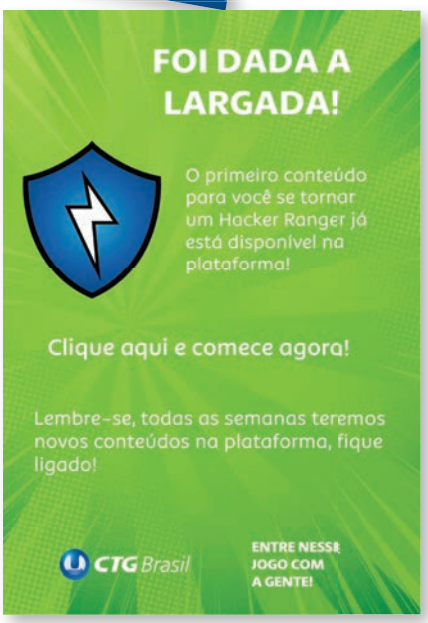
CAMPANHA DE LANÇAMENTO DO PROJETO ENVIADA POR E-MAIL PARA OS PROFISSIONAIS:

Com o intuito de aproximar os profissionais, os dois personagens remetem a pessoas reais, respectivamente ao analista de Segurança de Informação que gerenciou o projeto, Gilson Henrique Silva e à diretora de Marca, Comunicação e Sustentabilidade, Salete da Hora. Foi o próprio Gilson quem criou os desenhos.









A adesão ao programa é voluntária, mas a nova estratégia de comunicação sensibilizou metade dos colaboradores no lançamento, com cerca de 500 adesões e mais de mil interações (detalhes no item "Resultados"). Menos de um mês depois do lançamento da plataforma, os profissionais administrativos passaram a trabalhar em casa devido à pandemia. A comunicação foi intensificada e a participação no *Hackers Rangers* acabou se tornando mais um canal de comunicação e interação entre os funcionários.

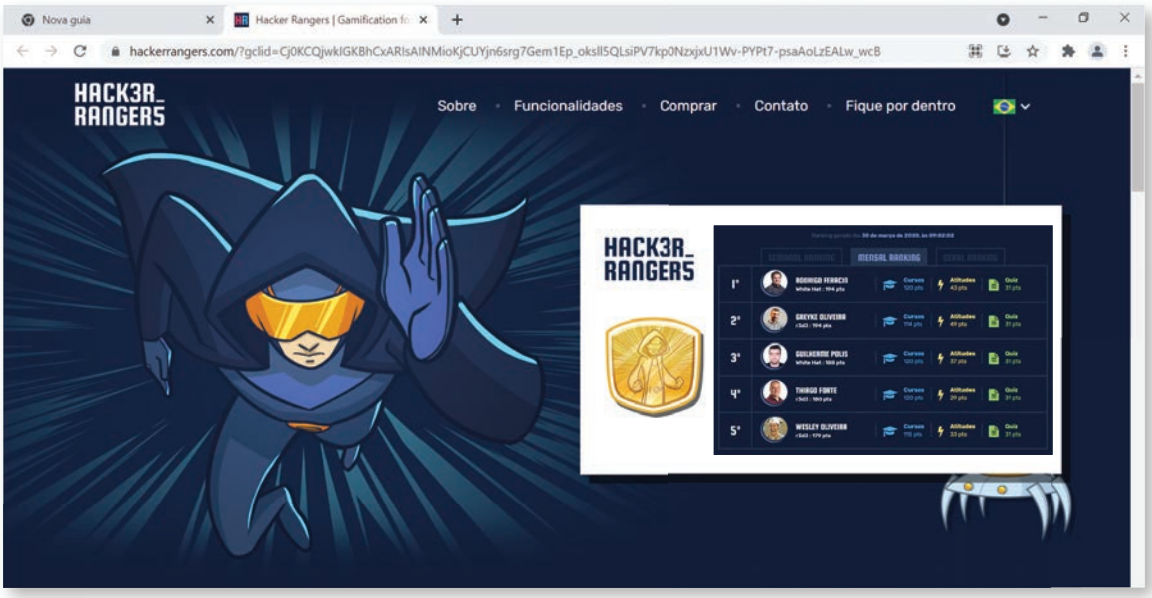
PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Foram diversas frentes desenvolvidas ao mesmo tempo para a criação do programa que foi dividido em duas fases. Na primeira, foi utilizada a plataforma *Hacker Rangers*, de jogos sobre segurança digital e que foi devidamente adaptada para as necessidades da CTG Brasil. Nela, o profissional da empresa podia participar de treinamentos, quizzes, e outros conteúdos, além de acompanhar sua performance através de um ranking. Na segunda, foi escolhida uma nova plataforma. O programa ganhou uma web serie, foram criados grupos entre os departamentos para aumentar a cooperação. Em ambas as fases foram oferecidas lives com especialistas para aumentar a interatividade. Durante a primeira fase, o jogo teve como plano de fundo e personagens o mundo dos super-heróis, em temática bastante semelhante às histórias da Marvel, uma espécie de patrulha galáctica. Para isso, foi utilizada uma plataforma já existente.

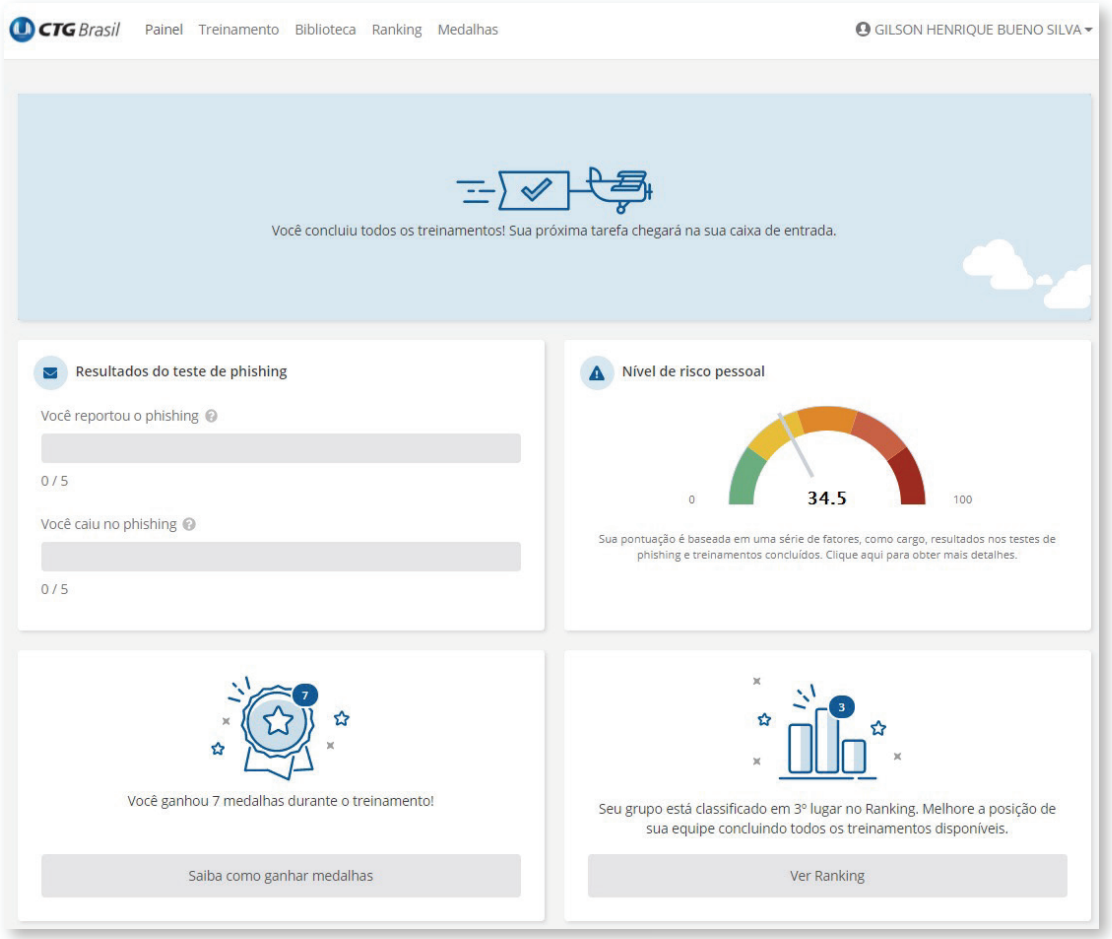
Levando em conta a dinâmica da segurança digital, as mudanças na rotina das pessoas e dos negócios ao longo da pandemia e considerando que a iniciativa se tornou benchmarking interno no grupo GTG como um todo, a CTG Brasil decidiu que, em 2021, iria além. Neste ano, o jogo começou sua segunda fase com novos cenários, novos desafios e novos recursos.

Com o avanço do programa, a empresa constatou que não era possível manter a segurança das informações sem o apoio e olhares atentos de todos os profissionais, então foi disponibilizado um canal direto para reportar e-mails maliciosos, que é o método mais comum para iniciar ataques as organizações. Com um simples clique em um botão no próprio Outlook, o profissional da CTG Brasil consegue enviar um e-mail suspeito para a análise da equipe de Segurança da Informação da CTG Brasil.

Ao entrar no sistema atual, o profissional da CTG Brasil encontra uma tela com dados sobre a performance dele no jogo como número de tarefas concluídas e a concluir, quantas vezes ele reportou ou caiu em armadilhas virtuais (*phishing*), suas medalhas e pontos ganhos, a performance do setor em que ele trabalha, seu histórico de conquistas, além dos treinamentos, vídeos e conteúdos diversos e ainda os quizzes feitos e a fazer.



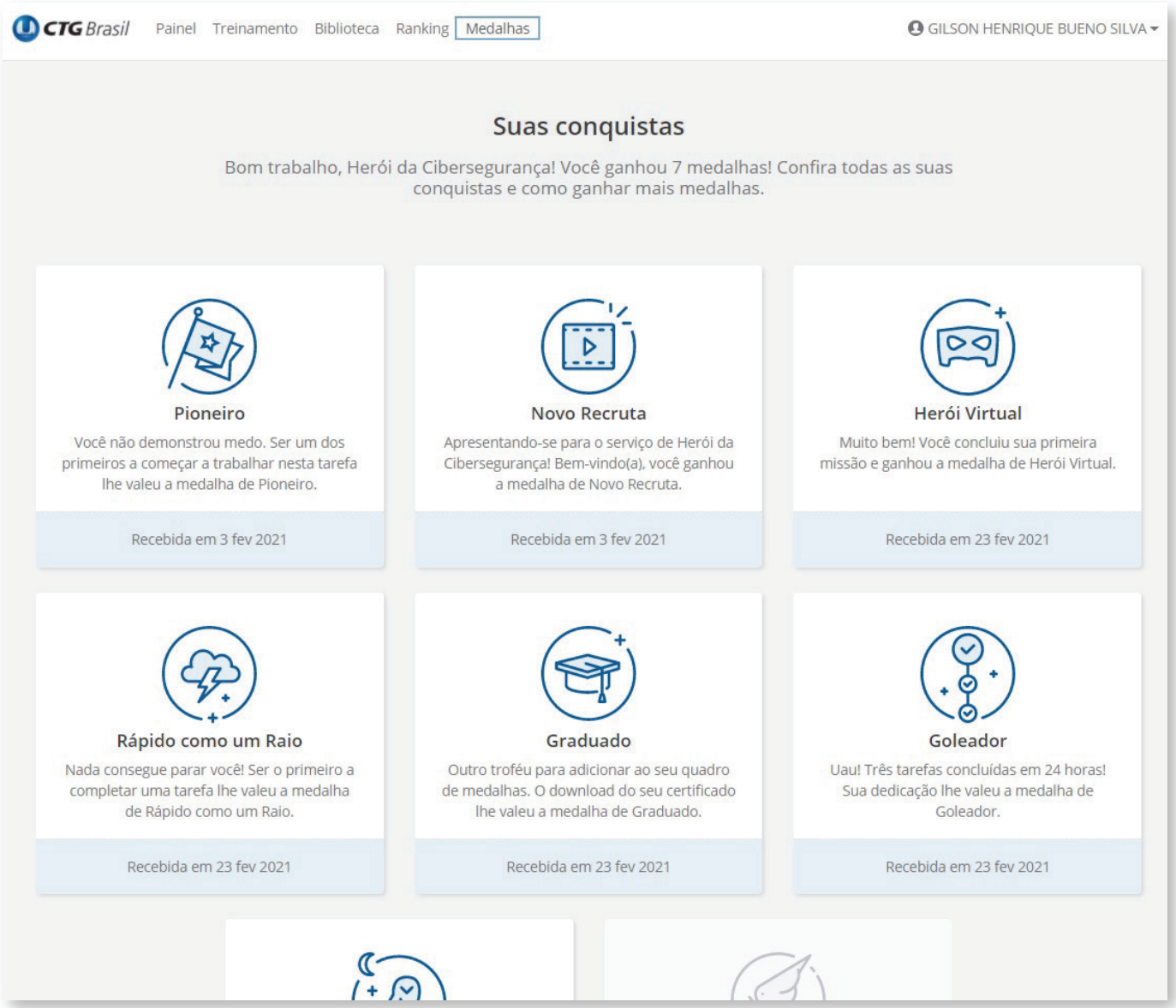
Plataforma Hacker Rangers, 2020



Plataforma Knowbe4 2021



Plataforma Knowbe4 2021



Plataforma Knowbe4 2021



A plataforma mostra ainda um termômetro com o nível de risco de cada profissional para a segurança da informação da empresa. Esse termômetro, atualizado diariamente, considera diversos critérios como o nível de acesso à informação daquele colaborador, a área em ele trabalha e o comportamento digital dele nas ferramentas da empresa diante das armadilhas virtuais simuladas pela empresa, além de dados vazados na internet, bem como sua participação no programa.

Para estimular a participação contínua, a cada semana a plataforma tem novidades.
O colaborador recebe por e-mail convites para um treinamento novo, ou outras atividades.
Todos os conteúdos podem ser acessados a qualquer momento. Tudo é conduzido pelos dois personagens-símbolo da campanha.

No final de cada temporada são enviados comunicados mostrando os vencedores da saga naquele período. São divulgados rankings semanais, mensais e um apanhado geral desde o início do programa.
A comunicação se dá por e-mail e pela intranet. Ela é enviada a todos os funcionários – mesmo aqueles que não aderiram à campanha – com o intuito de incentivar o crescimento contínuo das adesões. Também pontua quem convence um colega a participar.

Além dos temas já mencionados, foram trabalhadas questões como senhas seguras, cuidado com a exposição de dados, dentre outros. O que aumentou o dinamismo do projeto foi o constante acompanhamento da equipe da CTG Brasil em relação aos novos golpes que surgiam ao longo da pandemia. Semanalmente são disponibilizados conteúdos mostrando os "últimos lançamentos" em armadilhas virtuais.
Para isso, as equipes de Comunicação e TI estão constantemente vigilantes sobre os novos golpes que aparecem no mercado.

Com as pessoas trabalhando em casa, o escopo de temas abordados pelo programa aumentou. A ideia foi levar os conceitos para além do colaborador e atingir toda a família. Assim, temas ligados a redes sociais, compras on line e entretenimento ganharam espaço.

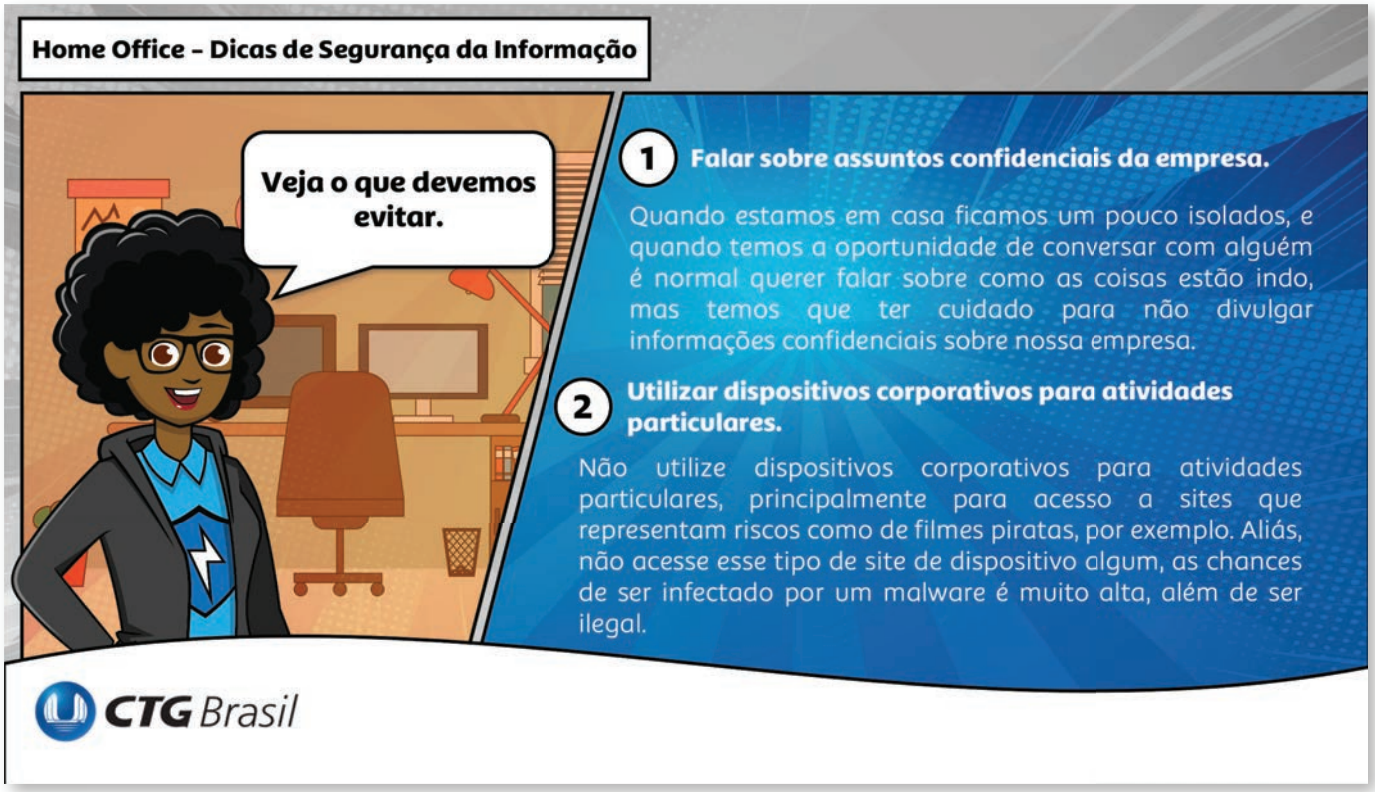


Logo nas primeiras semanas da pandemia – quando as pessoas foram orientadas a não sair de casa – apareceram diversos golpes virtuais ligados a ofertas como assinatura gratuita da plataforma de streaming Netflix ou falsas lojas on line. Imediatamente foram produzidos conteúdos alertando sobre esses problemas e disponibilizados no sistema para conhecimento de todos.

Todo o conteúdo é produzido de maneira leve, com visual atraente e em linguagem divertida. Infográficos e quadrinhos são recursos frequentes nas peças de comunicação. Aos poucos foram incorporados itens relacionados à segurança física, principalmente em relação a documentos e registros físicos de dados pessoais e da empresa.







Engenharia Social

O termo *phising* surgiu no universo cibernético a partir de um trocadilho com *fishing*, que em inglês significa pescaria. Por isso, na segunda fase os super-heróis se transformaram em corajosos marujos enfrentando os mares revoltos da segurança da informação, evitando pescarias indesejadas. O símbolo da campanha também mudou. O escudo de super-herói se transformou em uma isca de pesca.



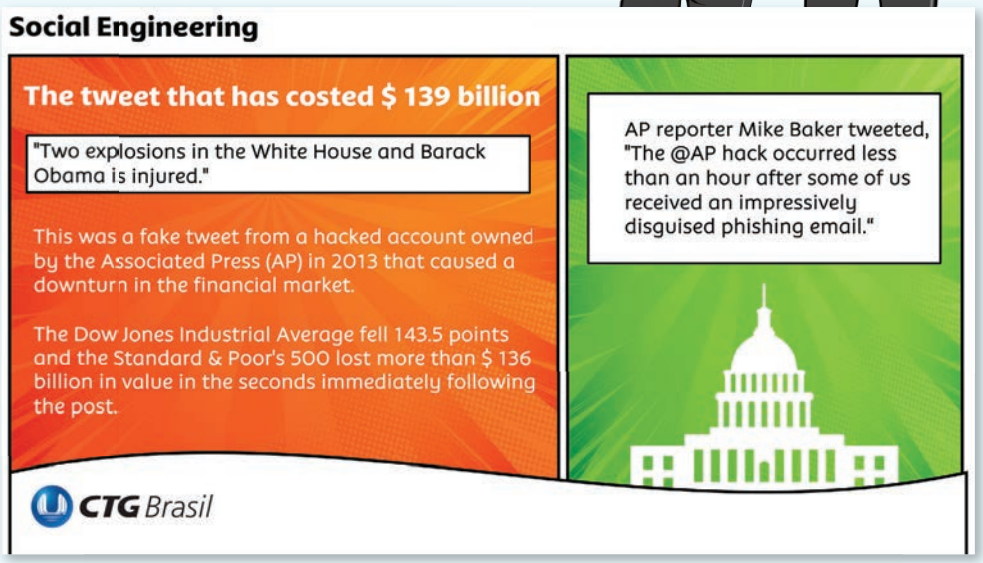
Os símbolos da campanha em 2020 e 2021



Marujos em 2021



Rangers em 2020

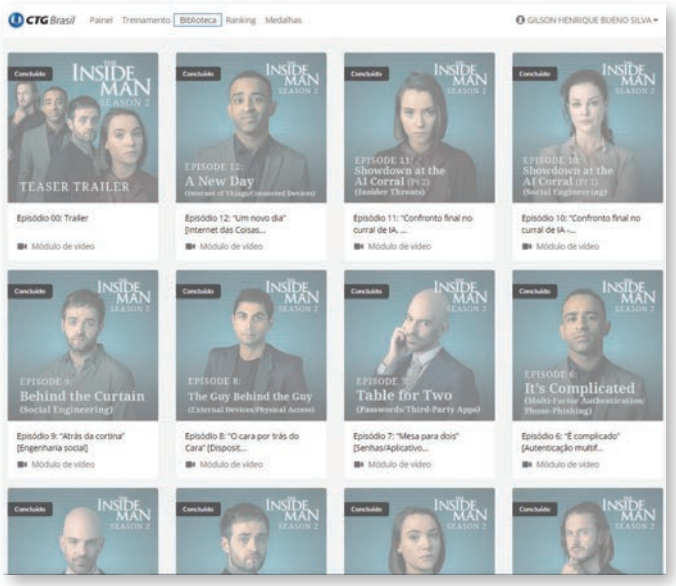


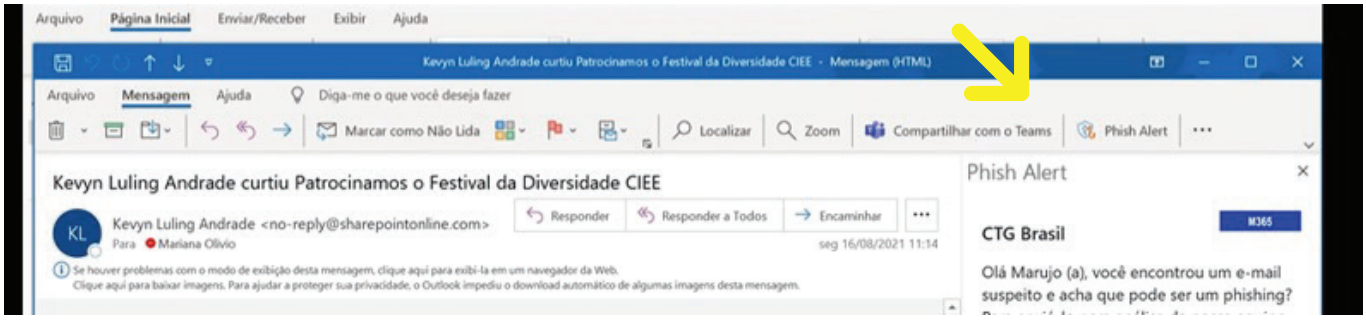
> Ao analisar a primeira fase do projeto notamos alguns elementos que nos nortearam para desenhar este segundo momento. O primeiro ponto que consideramos importante era que o jogo estava entrando em uma nova fase, então um novo cenário poderia ajudar. Queríamos também aumentar o acesso em outros idiomas além do português e do inglês. E, em termos de conteúdo precisávamos dar ênfase ao phising, que são as armadilhas virtuais que buscam induzir os usuários a clicar em *links* maliciosos ou passar informações confidenciais.
>
> **Gilson Henrique Silva**
> Analista de Segurança da Informação e principal articulador do projeto

SEGUNDA FASE

Parcialmente reformulado, o Programa de Conscientização em Segurança da Informação chegou em 2021 mais desafiador também. Foram intensificadas as lives com especialistas internos e externos, cuja gravação poderia ser assistida posteriormente, mas a participação ao vivo melhoraria a pontuação. Além das *lives*, os vídeos produzidos pelos próprios profissionais de TI da empresa ganharam mais destaque, bem como a web serie *The Inside Man*, uma produção internacional voltada para alertas de segurança da informação por meios de simulações de situações cotidianamente vividas em empresas. A nova plataforma expandiu geograficamente o projeto, pois permite a tradução do material para diversos idiomas, inclusive mandarim, que é o idioma de origem do grupo CTG.

A empresa também intensificou a produção de falsos *phishings* para testar quem iria cair nas armadilhas ou quem perceberia e denunciaria. Passou a criar e-mails falsos enviados para todos os colaboradores, independentemente de estarem ou não participando do programa. Nesses casos, todos que caem no *phishing* são direcionados na hora a um rápido treinamento sobre aquele determinado risco para o qual ele não teve atenção. Esse treinamento é obrigatório, mesmo para aqueles que não aderiram à plataforma. Para facilitar, há no próprio sistema de e-mails da empresa, um botão para reportar para a área de TI qualquer *phishing* detectado. Para incentivar as denúncias de phishings e atitudes suspeitas, a área de TI responde individualmente cada mensagem enviada, informando o resultado da investigação.





O programa desde o início incentiva as chamadas ciberatitudes que são mudanças de hábitos dos colaboradores e de suas famílias. Elas podem ser reportadas com evidências na plataforma e servir como exemplo para todos.



"As ciberatitudes são muito importantes nesse processo porque mostram que o profissional foi além do teórico, além de receber uma informação em um treinamento ou em uma peça de comunicação e responder um questionário para saber se ele memorizou ou não. Por isso, damos valor para as evidências das mudanças de atitude fora da plataforma do game. O colaborador que alterou algum hábito digital pode fazer upload de fotos na plataforma ou outras evidências dessa mudança que elas também são reconhecidas como conquistas"

Outra novidade trazida na segunda fase é o reconhecimento por equipes. "Notamos que seria possível utilizar a plataforma para ir além da conscientização sobre segurança da informação. Com tanta gente trabalhando em casa em função da pandemia, ela poderia ser mais um meio de aproximação entre os colaboradores. O reconhecimento das equipes ajudou a aumentar a interatividade tanto dos colaboradores com a plataforma quanto dos colaboradores em si, porque agora um incentiva o outro a participar assim o departamento pontua melhor e é reconhecido por isso"

Salete da Hora
Diretora de Marca, Comunicação e Sustentabilidade



Inicialmente, a inclusão do reconhecimento por grupos trouxe uma certa preocupação para a equipe da CTG Brasil quanto ao risco de se cometer algum tipo de injustiça, pois como a adesão é voluntária corria-se o risco de ter áreas participando de maneira mais robusta que outas, e de determinadas áreas, pelas suas próprias características, terem colaboradores com mais facilidade em assimilar os conteúdos sobre segurança da informação do que outras.

> "Mas isso foi resolvido no estabelecimento dos critérios de pontuação, que foram minuciosamente elaborados para corrigir tais desvios, dando equilíbrio aos grupos que participassem com a mesma intensidade, mesmo diferindo na quantidade de membros ou em familiaridade com o tema."
>
> **Gilson Henrique Silva**
> Analista de Segurança da Informação e principal articulador do projeto

> "O programa de conscientização de segurança da informação é um dos principais pilares da nossa estratégia de cibersegurança. O trabalho realizado pela TI em conjunto com a área de Comunicação trouxe um conteúdo muito rico e importante para todos os funcionários da empresa, de forma leve e inovadora. Através da gameficação atingimos um alto nível de engajamento."
>
> **Flaviano Sousa**
> Diretor de TI da CTG Brasil



Investimento

O programa foi feito basicamente com recursos humanos internos, contando com apoio de fornecedores em itens bastante específicos. Pelos resultados apresentados e pelo engajamento do público, o retorno sobre investimento foi considerado pela CTG Brasil como de grande eficácia.

INVESTIMENTOS		
VALOR R$	AÇÕES COBERTAS	ORIGEM DOS RECURSOS
30.000,00	Concepção, preparação do sistema e primeira temporada (2020)	Internos CTG
54.540,00	Revisão da plataforma e segunda temporada (até agosto de 2021)	Internos CTG
12.026,00	Vales-presente, brindes e divulgação	Internos CTG
96.566,00	**TOTAL**	

Resultados

A campanha trouxe resultados crescentes tanto no engajamento da equipe quanto no aumento de atitudes seguras no dia a dia. A tabela abaixo mostra alguns dados quantitativos, mas a maior satisfação da CTG Brasil é perceber que está mudando a vida das pessoas tornando-as mais seguras no trabalho e em casa, atingindo toda a família como mostram algumas das ciberatitudes tomadas ao longo do programa e que exemplificamos a seguir.

PROGRAMA CONSCIENTIZAÇÃO - CRESCIMENTO		
	2020	AGOSTO 2021
Participantes	1196	1200
Quantidade de acessos	10354	12101

NÚMEROS TOTAIS	
CONTEÚDOS PRODUZIDOS ATÉ AGOSTO 2021	198
Total de acessos	22.455
Quizzes respondidos	1871
Phising reportados	1279
Ciberatitudes registradas	1847
Ameaças reais reportadas	732

Com a palavra, os jogadores



"Como diretor Financeiro, tenho como atribuição principal, defender o dinheiro da companhia. E posso dizer com segurança que hoje, o crime digital é uma das modalidades que mais coloca em risco o capital financeiro, tanto de nossa empresa quanto da maioria do mercado. Neste sentido, o Hackers Rangers ajuda muito: ele é um programa inovador que cria consciência quanto as boas práticas inerentes a Segurança da Informação, ajudando a "fechar portas" onde os criminosos digitais poderiam entrar."

Carlos Nakao
Diretor Financeiro



"Esta semana fizemos uma 'varredura' no celular e no computador da minha mãe. Como ela é professora, neste período de quarentena, tem procurado muito conteúdo pela internet e como toda boa 'mãe,' clica em tudo. Explicamos todos os cuidados necessários e que não é todo conteúdo que é confiável." Ana Maria Borges – Analista de Gestão de Projetos
"Nunca havia trocado a senha do wi-fi de casa, e logo após o vídeo desta semana entendi a importância e troquei. Obrigada pelas dicas!"

Thamyres Maria Viana Arantes
Assistente de Serviços Administrativos



"Recebi um e-mail com conteúdo parecendo ser verdadeiro, porém, o endereço remetente era estranho e o link dentro do corpo da mensagem também direcionava a site desconhecido e que não batia com o endereço do remetente na web. Para ver a veracidade da mensagem acessei diretamente a plataforma onde tenho feito cursos e tive as confirmações corretas. Preferi não acessar o link do e-mail recebido".

Aparecido Dos Santos Bezerra
Técnico de Manutenção Eletroeletrônica Sênior



"Hoje me desloquei até a usina e notei que, na lousa (quadro) da sala de operação havia uma senha anotada. Falei para o operador que estava na escala que aquela prática não é indicada, senão proibida quando se trata de senhas que poderiam dar acesso a dados corporativos. Sugeri que apagasse. Há pouco tempo fui até lá de novo e vi que a referida anotação foi apagada do quadro".

Rodrigo Henrique Garcia Rodrigues
Analista de Suporte Técnico



"Recebi uma mensagem de texto dizendo que havia ganhado alguns prêmios e, para dar continuidade no recebimento, deveria responder à mensagem enviando alguns dados particulares. Não respondi a mensagem e não forneci meus dados, além de bloquear o número".

João Paulo Nascimento Ferreira
Técnico de Manutenção Mecânica Júnior



"Hoje caminhando pela galeria da usina encontrei um crachá de um colega terceirizado, logo lembrei do curso a respeito de segurança física, procurei o profissional que eu reconheci pela foto e entreguei a ele. Ele ainda não tinha percebido havia deixado cair. Esse fato poderia ocorrer fora da usina e, caindo em mãos erradas, causar certo transtorno".

Aliffer Dutra
Técnico de Manutenção Mecânica Júnior