GAMIFICAÇÃO APLICADA A PROGRAMAS E CAMPANHAS DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

GAMIFICATION APPLIED TO INFORMATION SECURITY AWARENESS PROGRAMS AND CAMPAIGNS

Rodolpho Andreazza Marinho, Fatec Ministro Ralph Biasi - Americana, rodolpho.marinho@fatec.sp.gov.br
Jonas Bodê, Fatec Ministro Ralph Biasi - Americana, jonas.bode@fatec.sp.gov.br

Resumo

O fator mais determinante no sucesso ou fracasso da segurança dos ativos de informação nas organizações é o fator humano. Os sistemas modernos estão cada vez mais seguros devido aos anos de desenvolvimento na área da segurança da informação. Estudos têm mostrado que a falta de conscientização dos usuários, referente aos perigos das suas ações e das ameaças no contexto da tecnologia da informação, levam a uma maior ocorrência de incidentes de segurança. Os programas e campanhas de conscientização de segurança da informação apresentam-se como uma solução para o problema. Contudo, as abordagens e métodos tradicionais desses programas e campanhas vêm se mostrado insuficientes para conscientizar e gerar comportamentos seguros de seus usuários. Nesse sentido, este trabalho tem por objetivo verificar a eficácia da gamificação em ações de conscientização de segurança da informação. Para tanto, utilizou-se de uma pesquisa bibliográfica, exploratória, descritiva com abordagem quantitativa, além da utilização do jogo eletrônico Kahoot!. Para viabilizar a coleta dos dados foi aplicado um questionário. Os participantes foram discentes da Faculdade de Tecnologia de Americana Ministro Ralph Biasi. Os dados foram analisados utilizando estatística básica. Este estudo mostra que o uso do *software* Kahoot! proporcionou resultados positivos, tendo em vista que os alunos que participaram do jogo tiveram um melhor desempenho em 66% das questões abordadas. Dessa forma, a gamificação é mais uma ferramenta que pode ser utilizada em ações de treinamento e conscientização em segurança da informação.

Palavras-chave: Segurança da Informação, Conscientização de Segurança Cibernética, Gamificação.

Abstract

The most determining factor in the success or failure of information asset security in organizations is the human factor. Modern systems are increasingly secure due to years of development in the field of information security. Studies have shown that users' lack of awareness of the dangers of their actions and threats in the context of information technology leads to a greater occurrence of security incidents. Information security awareness programs and campaigns present themselves as a solution to the problem. However, the traditional approaches and methods of these programs and campaigns have been shown to be insufficient to raise awareness and generate safe behaviors among their users. In this sense, this work aims to verify the effectiveness of gamification in information security awareness actions. For that, it was used a bibliographical, exploratory, descriptive research with a quantitative approach, in addition to the use of the electronic game Kahoot!. To enable data collection, a questionnaire was applied. The participants were students of the Faculty of Technology of Americana Ministro Ralph Biasi. Collected data was analyzed using basic statistics. This study shows that using

Kahoot! provided positive results, considering that the students who participated in the game performed better in 66% of the questions addressed. Thus, gamification is another tool that can be well used in training and awareness actions in information security.

Keywords: Information Security, Cyber Security Awareness, Gamification.

1. Introdução

Kevin Mitnick, em entrevista à CNN, disse que uma companhia pode gastar centenas de milhares de dólares com firewalls, sistemas de detecção de intrusos, encriptação e outra tecnologias de segurança, mas se um criminoso fizer uma ligação para uma pessoa de confiança da companhia e se essa pessoa obedecer, entregando o acesso, então todo o dinheiro gasto em tecnologia é desperdiçado (ABREU, 2000).

O aumento mundial de incidentes de segurança de tecnologia da informação se deve principalmente ao aumento de dispositivos móveis, ao aumento de dados eletrônicos transmitidos, ao aumento de grupos organizados de crimes cibernéticos, dificuldade de rastrear os invasores cibernéticos e conhecimento limitado de segurança de informação entre os usuários da Internet (ALOUL, 2012).

É notório que a prevenção é melhor do que o remédio. O único meio para os usuários das tecnologias de informação tomarem atitudes seguras e preventivas é através da conscientização das ameaças e riscos presentes no contexto de segurança da informação (SI), que provoque mudanças de atitude e de comportamento (ALOTAIBI, 2016).

Vários autores que tratam de conscientização de segurança da informação relatam que os métodos das campanhas e programas atuais são muitas vezes insuficientes para levar o usuário a um nível adequado de conscientização de segurança da informação e/ou usuários já possuem conhecimento das ameaças pertinentes de SI, contudo não tomam atitudes preventivas. Vários estudos têm mostrado uma relação positiva entre conscientização de segurança da informação com a prevenção de incidentes de segurança (ABAWAJY 2014; BADA *et al*, 2019; SZWILLING, 2022).

Estudos e pesquisas na área de educação e psicologia têm mostrado que a gamificação é uma boa ferramenta didática que cria possibilidades para aprendizagens mais engajadoras e promove mudança de hábitos e comportamentos (ZICHERMANN, 2011; KAPP, 2012; ALOTAIBI, 2016).

Rigby (2015) cita a motivação como um dos principais desafios para a conscientização e treinamento de segurança da informação. Já Rhee *et al*. (2011) apontam a mudança de comportamento como o objetivo da conscientização e treinamento de segurança da informação.

Na literatura não foram encontrados estudos com abordagem quantitativa sobre a eficácia da gamificação em ações de conscientização de segurança de informação. Nesse sentido, o presente trabalho tem como objetivo explorar esse aspecto, apresentando resultados numéricos sobre o emprego do *software* didático Kahoot! no processo ensino-aprendizagem em segurança da informação.

2. Referencial Teórico

2.1 Conscientização no contexto de Segurança da Informação

A publicação especial NIST 800-16 (1998) define conscientização de segurança da informação como uma atividade separada do treinamento. O objetivo das apresentações de conscientização é simplesmente focar a atenção na segurança. As apresentações de conscientização destinam-se a permitir que os indivíduos reconheçam as preocupações de segurança da tecnologia da informação (TI) e respondam de acordo" (WILSON, 1998).

Shaw *et al*. (2009) definiram conscientização de segurança da informação, ou seja,

segurança cibernética como: “O grau de compreensão dos usuários sobre a importância da segurança da informação, suas responsabilidades e atuação para exercer níveis suficientes de controle de segurança da informação para proteger os dados e as redes da organização”.

A conscientização consiste na ação de tomar conhecimento sobre algo, modificando hábitos e comportamentos. Na verdade, o construto denominado conscientização das ameaças cibernéticas emergiu do modelo do processo de difusão da inovação que define conscientização como a medida em que os potenciais usuários estão conscientes de uma inovação e têm uma percepção geral de seus atributos (ROGERS, 1983).

Além desses trabalhos, outras pesquisas têm mostrado que a conscientização reduz os incidentes de segurança da informação (SHAW *et al*, 2009; MCCROHAN *et al*, 2010; MORE, 2011; ALAOUL, 2012; SAS *et al* ,2021; HWANG 2021).

2.2 Programas de Conscientização

Um programa de conscientização de segurança de TI bem-sucedido consiste em: 1) Desenvolver uma política de segurança de TI que reflita as necessidades de negócios ponderada por riscos conhecidos; 2) Informar os usuários de suas responsabilidades de segurança de TI, conforme a documentação de política e procedimentos de segurança da agência; 3) Estabelecer processos para monitorar e revisar o programa de conscientização (WILSON, 2003).

Portanto, não é possível elaborar um programa de conscientização sem antes desenvolver uma política de SI. Uma política de segurança da informação é um conjunto de regras e normas claras, para funcionários guardarem e protegerem a informação e definir controles efetivos contra ameaças (FONSECA, 2009).

Um dos principais objetivos de uma política de segurança da informação é definir os direitos e responsabilidades dos usuários dos recursos de informação. Uma política de segurança da informação eficaz ajudará os usuários a entenderem o que é um comportamento aceitável e responsável em relação a esses recursos para garantir o manuseio seguro das informações em suas tarefas diárias. De fato, para ser totalmente eficaz, a política de segurança da informação precisa incorporar tanto as necessidades dos usuários, por informações precisas e confiáveis, quanto às necessidades do negócio, para atingir seus objetivos estratégicos (HÖNE *et al*, 2002).

Se a tomada de consciência sobre um determinado fato não leva à mudança de comportamento, então o processo de conscientização falhou em algum ponto. Por exemplo, mesmo que um colaborador tenha consciência de ameaça de *phishing*, mas não tome atitudes preventivas, ou seja, verificar a autenticidade de um *e-mail*, não clicar em links suspeitos e/ou baixar arquivos suspeitos, ele não tomou consciência da relevância, da possibilidade e das consequências da ameaça (SHAW, 2009).

2.3 Mudança de Comportamento

Flowerday *et al*. (2016) apontou que a Teoria do Comportamento Planejado (AJZEN, 1991) é a principal teoria para entender a intenção comportamental dos funcionários em cumprirem uma política de segurança da informação de uma organização. Essa teoria explica que a intenção de um indivíduo em assumir um determinado comportamento é influenciada por crenças normativas e normas subjetivas, crenças de controle e controle comportamental percebido, intenção comportamental e comportamento (AJZEN, 1991).

Crenças normativas são formadas pela percepção individual através pressões normativas sociais ou de crenças de pessoas sobre quais comportamentos devem ou não ser assumidos. Normas subjetivas são a percepção de um indivíduo sobre um comportamento específico que é influenciado pelo julgamento de outras pessoas importantes para o

indivíduo, como, por exemplo, pais, cônjuge, amigos, professores (AJZEN, 1991).

Crenças de controle são as crenças de um indivíduo sobre a presença de fatores que podem facilitar ou dificultar que assuma determinado comportamento. Controle comportamental percebido é a facilidade ou dificuldade percebida de uma pessoa em assumir um comportamento específico (AJZEN, 1991).

A intenção comportamental é a prontidão de um indivíduo para assumir um determinado comportamento. Supõe-se que essa intenção seja um antecedente imediato do comportamento. Baseia-se na atitude em relação ao comportamento, norma subjetiva e controle comportamental percebido, com cada preditor ponderado por sua importância em relação ao comportamento e às pessoas de interesse (AJZEN, 1991).

Por fim, o comportamento é a resposta observável de um indivíduo em uma determinada situação em relação a um determinado fato. Ajzen (1991) define o comportamento como uma função de intenções e percepções compatíveis de controle comportamental. Espera-se que o controle comportamental percebido modere o efeito da intenção sobre o comportamento, de modo que uma intenção favorável produz o comportamento apenas quando o controle comportamental percebido é forte (AJZEN, 1991).

Usando a Teoria do Comportamento Planejado, certos passos podem ser seguidos nos esforços para aumentar as chances de mudança de comportamento (AJZEN, 1991). Por exemplo, um programa de conscientização ou treinamento de segurança da informação específica, conjuntamente, ação, alvo e contexto. O programa solicita a colaboradores da organização que somente façam logins em suas estações de trabalho utilizando suas próprias credenciais e, ao término das atividades, façam *log-off*.

Quando um objetivo é especificado, uma fase de entrevistas pode ser usada para identificar os fatores que influenciam o seu alcance. As entrevistas ajudam a identificar resultados comportamentais relevantes, referentes aos fatores culturais, fatores facilitadores e barreiras à mudança no comportamento e na população alvo (GLANZ *et al*, 2015).

O trabalho de revisão sistemática e análise de Krath *et al* (2021) apontou a Teoria do Comportamento Planejado como fundamentação teórica da gamificação, como, por exemplo, jogos sérios e aprendizado baseado em jogo.

Outra teoria do comportamento muito pertinente é a Teoria da Autodeterminação. A Teoria da Autodeterminação é um processo de motivação com três estados emocionais: 1) motivação intrínseca, 2) motivação extrínseca e 3) desmotivação. A Teoria apresenta três necessidades psicológicas humanas essenciais: 1) competência, 2) autonomia e 3) relacionamento (DECI *et al*, 2000).

No contexto da Teoria da Autodeterminação, competência é a necessidade de sentir-se capaz de ter sucesso em alguma atividade. A autonomia é definida como o grau em que o indivíduo se identifica como responsável pelo início de uma atividade. Relacionamento é a necessidade de associar-se com outros e com o mundo social em geral (DECI *et al*, 2000).

A Teoria da Autodeterminação pode ser usada para prever e/ou estimular certo comportamento fazendo uso das três necessidades psicológicas humanas essenciais.

O trabalho de meta-análise de Sailer *et al*. (2019) demonstrou conexões entre Teoria da Autodeterminação e Gamificação. O trabalho concluiu que a gamificação traz efeitos positivos nos processos cognitivos, de aprendizagem, motivacionais e comportamentais, em um ambiente geral de aprendizagem.

2.4 Gamificação

O uso de mecânicas de jogos e pensamento de jogos (*game-thinking*) para engajar usuários a resolver problemas é a definição dada a gamificação por Zichermann e Cunningham (2011). A Gamificação pode ser prontamente aplicada a qualquer problema

que possa ser resolvido, influenciando a motivação e o comportamento humano (ZICHERMANN et al, 2011).

Por sua vez, Huotari e Hamari (2012) definiram gamificação como um processo de aprimoramento de serviços com mecânicas motivacionais para invocar experiências lúdicas e outros resultados comportamentais.

Mecânicas de jogos são missões, informações em cascata, quadros de líderes, metas, níveis, medalhas, dramatização, pontos, desafios e recompensas, dentre outros (ARNAB 2014).

É notório que jogos digitais vêm assumindo um papel cada vez maior na sociedade. Diversas plataformas de aprendizado utilizam elementos de jogos digitais e estratégias de jogos, como o Duolinguo, Matific, Kahoot!, dentre outros.

Duolingo é um site e aplicativo móvel de aprendizado de idiomas. Os usuários praticam vocabulário, gramática e pronúncia, usando repetição espaçada. Os exercícios podem incluir tradução escrita, compreensão de leitura e fala de histórias curtas. Em junho de 2021, o Duolingo ofereceu 106 cursos em 41 idiomas (DUOLINGUO, INC, 2022).

Matific é uma plataforma que possui uma coleção de jogos e atividades interativas na área de matemática para crianças em idade escolar, auxiliando-as a construir uma compreensão conceitual de várias habilidades fundamentais. Essa plataforma tem diversas atividades que podem ser pesquisadas por séries e tópicos. Além das avaliações, o conteúdo possui quatro formas: planilhas, episódios, problemas de palavras e oficinas. Os alunos podem preencher as planilhas on-line ou os professores podem imprimi-las. Para uma experiência mais aberta, os professores podem usar oficinas que apresentam linhas numéricas ou fatias de pizza para brincar com conceitos relacionados com números inteiros e frações (MATIFIC - EDUCATIONAL MATHS GAMES, 2022).

Kahoot! é uma plataforma de aprendizado baseada em jogos, usada como ferramenta educacional. Seus jogos de aprendizagem, "kahoots", são questionários de múltipla escolha, gerados pelo usuário, que podem ser acessados por meio de um navegador da web ou do aplicativo Kahoot!

O Kahoot! foi projetado para aprendizagem social, com os alunos reunidos em torno de uma tela comum, como um quadro interativo, projetor ou monitor de computador. O site também pode ser usado por meio de ferramentas de compartilhamento de tela, como Skype, Zoom ou Google Meet. O jogo é simples. Todos os jogadores se conectam usando um PIN, gerado e mostrado na tela comum. Geralmente um professor ou um líder de negócio, dentre outros, constrói um questionário com perguntas e respostas com o conteúdo a ser avaliado, cujos acertos podem ser premiados. O criador pode escolher se os jogadores podem obter de 0 até 1000 pontos ou de 0 até 2000 pontos. Os pontos que o jogador recebe consideram a velocidade da resposta e a pontuação da pergunta. Os pontos aparecem na tabela de classificação após cada resposta. O jogador também pode responder as questões em sequência para ganhar mais pontos (KAHOOT! ASA, 2019). O aplicativo permite também que em cada questão sejam adicionados vídeos, imagens e/ou músicas.

O princípio da gamificação pode ser facilmente exemplificado com as brincadeiras e recompensas que pais e educadores fazem com crianças. Por exemplo, brincar de “aviãozinho” com algum vegetal que uma criança não quer comer e/ou oferecer uma recompensa se ela comer todos os vegetais de seu prato (ZICHERMANN, 2011).

De acordo com Zichermann et al. (2011), ao transformar a experiência em um jogo, incluindo alguma recompensa por conquista, pode-se produzir uma mudança de comportamento sem precedentes. E quando o efeito é amplificado com um ciclo de prova social e *feedback* o céu é o limite para o “crescimento viral”. Crianças podem até mostrar a seus amigos como transformar brócolis em dopamina antes de ir atrás do bolo de chocolate.

Um método comum de gamificação é o uso de medalhas de conquista. Normalmente,

não há valor prático em receber uma medalha. No entanto, obter uma medalha cria uma sensação de satisfação porque tal recompensa reconhece o progresso e/ou a realização de um objetivo.

O simples uso das medalhas de conquista pode satisfazer as três necessidades psicológicas humanas essenciais da Teoria da Autodeterminação: satisfaz a necessidade de competência ao reafirmar que o indivíduo tem capacidade para alcançar seu objetivo; satisfaz a autonomia se ele tiver várias opções de modalidades de medalhas de conquista para escolher; e satisfaz a necessidade de relacionamento se as medalhas de conquista são compartilhadas socialmente. Outras mecânicas de jogos, como quadros de líderes e pontos, dentre outros, podem satisfazer uma ou até mais necessidades da Teoria da Autodeterminação.

O trabalho de revisão sobre gamificação de Hamari *et al* (2014), intitulado "*Does Gamification Work?"* concluiu que, de fato, a maioria dos estudos revisados apresentam efeitos/resultados positivos. No entanto, os estudos analisados sugerem que existem alguns fatores geradores de confusão. Em particular, os estudos trazem à tona duas questões principais: 1) o papel do contexto que está sendo gamificado e 2) as características dos usuários. Majuri e Hamari (2018) também concluíram que a maioria dos estudos apresentam resultados predominantemente positivos. No entanto, embora os resultados pareçam promissores, também há um número substancial de estudos com resultados nulos ou mistos. Os estudos qualitativos geralmente indicam experiências e resultados muito variados, mesmo quando a tendência geral dos resultados é positiva. Portanto, os trabalhos que relatam resultados positivos devem ser tomados com cautela.

3. Metodologia

De acordo com Richardson et. al. 1999, método é a regra ou maneira para se alcançar determinado objetivo e metodologia são os procedimentos usados por determinado método. Logo, ao realizar uma pesquisa é necessário estabelecer os procedimentos metodológicos para se alcançar os objetivos propostos.

Quanto à utilização dos resultados, esta pesquisa se classifica como "pesquisa aplicada" porque visa solucionar problemas específicos a partir de uma aplicação prática. Quanto aos seus objetivos ou fins, o presente trabalho é definido como pesquisa exploratória porque objetiva explorar a eficácia da gamificação em ações de conscientização e treinamento em segurança da informação, incluído pesquisa bibliográfica sobre o tema. Também é definida como pesquisa descritiva onde, após a coleta dos dados, são descritas as características do fenômeno em estudo. Quanto à natureza do método empregado, a abordagem é quantitativa e o procedimento técnico "levantamento" foi utilizado para viabilizar a coleta dos dados. Esse procedimento envolve o questionamento dos participantes da pesquisa cujo comportamento se deseja conhecer (GIL, 2002). Nesse contexto, o questionário eletrônico é composto por um conjunto de perguntas de múltipla escolha e o respondente deve escolher uma das alternativas.

A amostra considerada neste trabalho foi composta por 235 alunos dos cursos oferecidos pela FATEC de Americana, SP, os quais foram divididos em três grupos distintos, a saber:

1) Grupo 1 (G1): grupo de controle. Composto por 74 participantes, os quais responderam um questionário eletrônico que contém perguntas sobre segurança da informação;

2) Grupo 2 (G2): Grupo composto por 77 alunos que receberam uma cartilha sobre conscientização de segurança da informação. A cartilha trata de alguns fatos pertinentes à segurança de informação, como ataques de engenharia social, ataques de *Phishing*, ameaças de redes Wi-Fi públicas, criptografia e a diferença entre http e https. Após a leitura da

cartilha, além de uma avaliação do seu conteúdo, os entrevistados responderam exatamente às mesmas questões apresentadas ao Grupo 1 e na mesma ordem, permitindo maior grau de comparação entre os dados obtidos.

3) O Grupo 3 (G3), composto por 84 participantes, recebeu a mesma cartilha do Grupo 2 e também participou de um jogo Kahoot!. O jogo consiste de uma série de perguntas sobre segurança da informação que abordavam o mesmo conteúdo da cartilha. O objetivo da aplicação do jogo foi analisar o impacto da gamificação em campanhas de conscientização e treinamento em segurança da informação. Os alunos desse grupo também responderam ao mesmo questionário enviado aos Grupos 1 e 2.

Os participantes do Grupo 1 puderam acessar o questionário eletrônico através de *links* que foram disponibilizados aos alunos, os quais foram escolhidos aleatoriamente para evitar tendenciosidades que poderia resultar de uma distribuição sistemática. O Grupo 2 pôde acessar a cartilha e o questionário eletrônico da mesma forma.

Os participantes do Grupo 3 foram divididos em quatro grupos de mais ou menos 20, devido à limitação da capacidade do laboratório utilizado. Assim sendo, a apresentação da cartilha e a aplicação do jogo Kahoot! ocorreu em quatro dias diferentes nos laboratórios da Fatec de Americana, SP.

A pesquisa foi realizada durante o mês de setembro de 2022.

4. Análise e interpretação dos resultados

Foram coletados dados relativos a 235 alunos dos cursos oferecidos pela FATEC de Americana, SP. Não foram identificados, dentre os formulários devolvidos, ausência de repostas nas questões, sendo 74, 77 e 84 questionários dos Grupos 1, 2 e 3, respectivamente.

O formulário de perguntas enviado aos alunos é apresentado na Quadro 1. Após o preenchimento do questionário, os dados foram compilados e calculadas as porcentagens de acertos, os quais encontram-se dispostos no Quadro 1 e ilustrados na Figura 1. Nota-se que de seis das nove perguntas (66%), a cartilha didática auxiliou na assimilação dos conceitos e práticas de segurança da informação. Para essas questões, os alunos que participaram do jogo obtiveram um melhor desempenho, quando comparado à cartilha.

No entanto, as perguntas 3 e 4 envolviam a análise de dois e-mails, um verdadeiro e um falso, respectivamente, dispostos nas Figuras 2 e 3. O grau de acertos da questão 4 foi superior a 70%, contudo a cartilha e o jogo não tiveram impacto algum no ensino-aprendizagem. Por outro lado, no que se refere a questão 3, os alunos que participaram do jogo Kahoot! obtiveram um melhor desempenho, porém houve um elevado grau de erro (abaixo de 30% de acertos). Além dessas duas perguntas, a cartilha e o jogo foram ineficientes na resolução da questão 5 e 7, as quais abordam a melhor forma de proteger as contas (de sites e aplicativos) de ataque de engenharia social, respectivamente. Nesses casos, é necessário realizar a abordagem de forma diferente com vistas a melhorias no processo de conscientização em segurança da informação.

Cabe ressaltar que o público da pesquisa foi de estudantes de graduação que possuem maior poder de cognição, bem como mais experiência em responder questões.

Quadro 1: Questionário e porcentagem de acertos por grupo

Questões	Acertos (%)		
	G1	G2	G3
1) Suponha que você está trabalhando em uma organização e você recebe uma ligação de alguém que diz ser do suporte de TI da sua empresa. A pessoa solicita que você use um programa de acesso remoto e insira uma chave numérica para que ela possa acessar o seu PC para uma	49%	66%	74%

manutenção. Essa ocorrência se trata de um? ( ) Ataque hacker ( ) Ataque de engenharia social ( ) Manutenção legítima			
2) Por que você deveria evitar utilizar redes Wi-Fi públicas, especialmente se você estiver lidando com suas informações pessoais identificáveis (finanças, bancos, redes sociais etc.) ( ) O maior perigo das redes Wi-Fi públicas é a capacidade de um hacker se posicionar entre você e o ponto de conexão. Então, em vez de se comunicar diretamente com a rede, você está enviando suas informações para o hacker que as repassa. ( ) Redes Wi-Fi públicas geralmente não tem boa infraestrutura para realizar comunicações importantes. Portanto, o ideal é evitar utilizá-las quando se pretende fazer algo importante (mexer com um aplicativo de banco, por exemplo) ( ) Hoje em dia a maioria das redes Wi-Fi são seguras devido aos avanços das tecnologias de Firewall, IDS e IPS.	39%	62%	68%
3) Na sua opinião, o e-mail abaixo é legítimo? Ver Figura 3 ( ) Sim ( ) Não ( ) Não sei	18%	14%	26%
4) Na sua opinião, o e-mail abaixo é legítimo? Ver Figura 4 ( ) Sim ( ) Não ( ) Não sei	81%	73%	81%
5) Qual é a melhor forma de proteger as suas contas de sites e aplicativos? ( ) Usar uma senha longa feita de várias palavras juntas ( ) Usar uma senha curta composta por vários caracteres especiais ( ) Usar uma senha gerada aleatoriamente por um gerenciador de senhas	59%	55%	53%
6) O que significa o "https://" no início de um URL, o endereço de um site, em oposição a "http://" (sem o "s")? ( ) Que o site é de alta definição ( ) Que a informação transmitida ao site é criptografada ( ) Que o site é atualizado ( ) Que o site é perigoso	45%	66%	75%
7) Cyber Criminosos acessam o computador de alguém e criptografam os arquivos e dados pessoais do usuário. O usuário não pode acessar esses dados, a menos que pague um resgate para decriptografar os arquivos. Essa prática é chamada de? ( ) Ataque Malware ( ) Ataque Ransomware ( ) Ataque de Engenharia Social ( ) Ataque DDoS	58%	57%	48%
8) “Navegação privada” é um recurso em muitos navegadores de internet que permite que os usuários acessem páginas da web sem que nenhuma informação (como histórico de navegação) seja armazenada pelo navegador. Os provedores de serviços de Internet podem ver as atividades online de seus assinantes quando esses assinantes estão usando a	38%	57%	72%

navegação privada? ( ) Sim ( ) Não			
9) Que tipo de riscos de segurança da informação pode ser minimizados usando uma Rede Privada Virtual (VPN)? ( ) Perda de anonimidade pelo provedor de internet ( ) Infecção de malware ( ) Uso de redes Wi-Fi inseguras ( ) Perda de sinal de internet	18%	35%	52%

Fonte: próprio autor

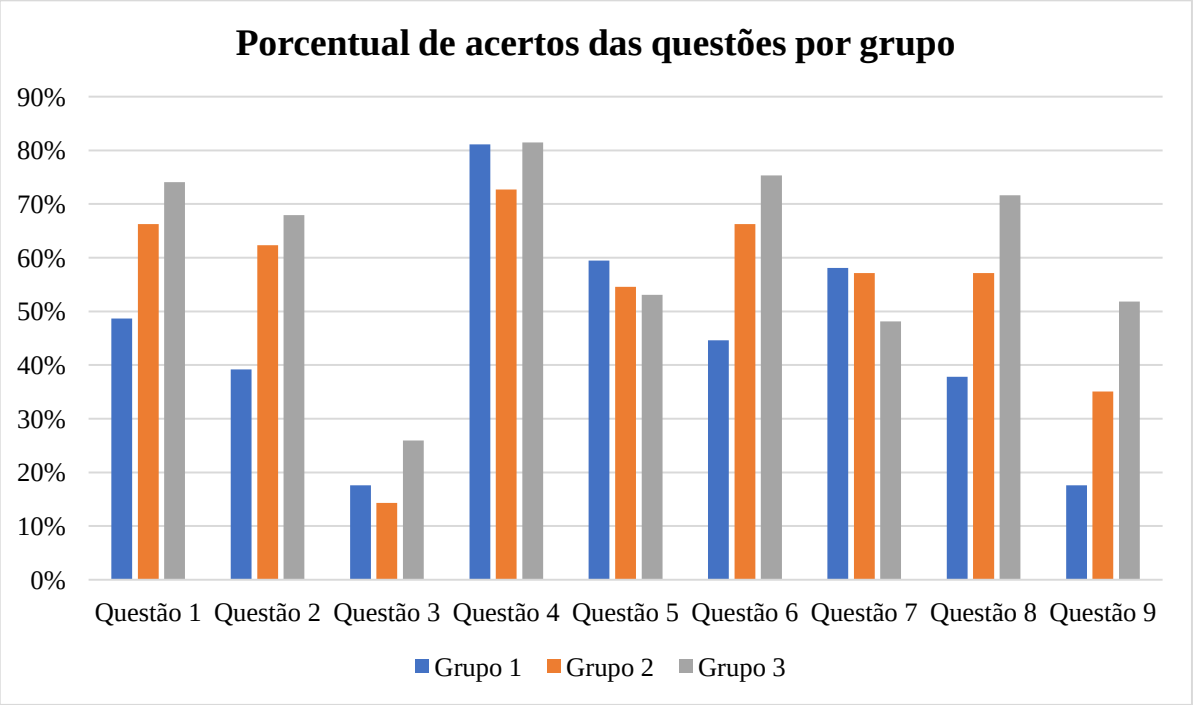

Figura 1: Gráfico do porcentual de acertos das questões por Grupo. **Fonte**: próprio autor.

Figura 2: E-mail da questão 3. **Fonte**: próprio autor.

Figura 3: E-mail da questão 4. **Fonte**: próprio autor.

5. Considerações finais

De acordo com a literatura, a gamificação é uma estratégia pedagógica que incorpora características e mecânica de jogos no processo de ensino-aprendizagem de modo a

aumentar o engajamento, a resolução de problemas e melhorar o aprendizado, motivando ações e comportamentos em ambientes educacionais ou empresariais.

A partir dessas considerações, o jogo Kahoot! foi utilizado neste trabalho com o intuito de engajar e melhorar ações e comportamentos em ambientes computacionais relacionados à segurança da informação.

Com a aplicação do questionário, foi possível obter resultados quantitativos em relação ao uso do jogo Kahoot! como meio de treinamento e conscientização de segurança da informação. A tendência geral dos resultados é positiva, tendo em vista que os alunos que participaram do jogo tiveram um melhor desempenho em 66% das questões abordadas.

Dada a tendência geral dos resultados obtidos, o jogo Kahoot! pode ser utilizado como meio de treinamento e conscientização de segurança da informação, considerando-se, evidentemente, ajustes no conteúdo e abordagem referente as questões com elevado grau de erro ou naquelas que a gamificação e a cartilha foram ineficientes.

Cabe ressaltar que o público da pesquisa foi de estudantes de graduação que possuem maior poder de cognição, bem como mais experiência em responder questões. Estudos futuro podem analisar melhor o impacto da gamificação como meio de treinamento e conscientização de segurança da informação em diferentes públicos e analisar mais concretamente o comportamento dos participantes em um ambiente de trabalho, antes e depois da aplicação da campanha/programa gamificada. Contudo, essa prática poderia ser uma abordagem muito invasiva.

Referências

ABAWAJY, J. User preference of cyber security awareness delivery methods. **Behaviour & Information Technology**, v. 33, n. 3, p. 237-248, 2014. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/0144929x.2012.708787 Acesso em: 13 abr. 2022.

ABREU, El.; Hacker K. M. Speaks out. Cable News Network, Atlanta, Georgia, 2000. Disponível em: http://edition.cnn.com/2000/TECH/computing/09/29/open.mitnick.idg/ Acesso em: 13 abr. 2022.

AJZEN, I. The theory of planned behavior. **Organizational behavior and human decision processes**, v. 50, n. 2, p. 179-211, 1991. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/074959789190020T Acesso em: 2 ago. 2022.

ALOTAIBI, Faisal et al. A review of using gaming technology for cyber-security awareness. **Int. J. Inf. Secur. Res.(IJISR)**, v. 6, n. 2, p. 660-666, 2016. Disponível em: https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf Acesso em: 21 abr. 2022.

ALOUL, F. A. The need for effective information security awareness. **Journal of advances in information technology**, v. 3, n. 3, p. 176-183, 2012. Disponível em: http://www.jait.us/uploadfile/2014/1218/20141218031904864.pdf . Acesso em: 13 abr 2022.

ARNAB, Sylvester et al. Mapping learning and game mechanics for serious games

analysis. **British Journal of Educational Technology**, v. 46, n. 2, p. 391-411, 2015. Disponível em: https://bera-journals.onlinelibrary.wiley.com/doi/abs/10.1111/bjet.12113 Acesso em: 16 ago. 2022.

BADA, M.; SASSE, A. M.; NURSE, J. R. C. Cyber security awareness campaigns: Why do they fail to change behaviour?. **arXiv preprint arXiv**:1901.02672, 2019. Disponível em: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf . Acesso em: 21 abr. 2022.

DECI, Edward L.; RYAN, Richard M. The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. **Psychological inquiry**, v. 11, n. 4, p. 227-268, 2000. Disponível em: https://www.tandfonline.com/doi/abs/10.1207/S15327965PLI1104_01 Acesso em: 10 ago. 2022.

DOLAN, Paul et al. MINDSPACE: influencing behaviour for public policy**. Institute of Government**, London, UK, 2010.Disponível em: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf . Acesso em: 15 abr. 2022.

DUOLINGUO, INC; What is Duolingo?; Disponível em: https://support.duolingo.com/hc/en-us/articles/204829090-What-is-Duolingo- Acesso em: 2 ago. 2022.

FLOWERDAY, S. V.; TUYIKEZE, T. Information security policy development and implementation: The what, how and who. **computers & security**, v. 61, p. 169-183, 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404816300670 . Acesso em: 2 ago. 2022.

FONSECA, P. F. Gestão de Segurança da Informação: o fator humano. **Pontifícia Universidade Católica do Paraná**. Curitiba, 2009. Disponível em: < https://www.academia.edu/download/53570328/Paula_Fernanda_Fonseca_-_Artigo.pdf> Acesso em: 2 ago. 2022.

GIL, A. C., Como elaborar projetos de pesquisa, 4ª Edição, Atlas, São Paulo, 2002 Disponível em https://docente.ifrn.edu.br/mauriciofacanha/ensino-superior/redacao-cientifica/livros/gil-a.-c.-como-elaborar-projetos-de-pesquisa.-sao-paulo-atlas-2002./view. Acesso em: 7 nov. 2022

GJERTSEN, Eyvind Garder B. et al. Gamification of Information Security Awareness and Training. In: **ICISSP**. 2017. p. 59-70. Disponível em: https://www.researchgate.net/profile/Maria-Bartnes/publication/314523152_Gamification_of_Information_Security_Awareness_and_Training/links/5ba3773ba6fdccd3cb652a88/Gamification-of-Information-Security-Awareness-and-Training.pdf . Acesso em: 13 abr. 2022.

GLANZ, K.; RIMER, B. K.; VISWANATH, K. (Ed.). Health behavior: Theory, research, and practice. **John Wiley & Sons**, 2015. p. 30-51. Disponível em: https://books.google.com.br/books?hl=pt-

BR&lr=&id=PhUWCgAAQBAJ&oi=fnd&pg=PR11&dq=Theory,+research,+and+practice+in+health+behavior.&ots=-erOfTEbHB&sig=7IIsGin_JjFEl7VIHNNydIbOwmc Acesso em: 10 ago. 2022.

HAMARI, J.; KOIVISTO, J.; SARSA, H. Does gamification work?--a literature review of empirical studies on gamification. In: 2014 **47th Hawaii international conference on system sciences**. Ieee, 2014. p. 3025-3034. Disponível em: https://ieeexplore.ieee.org/abstract/document/6758978/ Acesso em: 10 de agosto de 2022.

HERATH, T.; RAO, H. R. Protection motivation and deterrence: a framework for security policy compliance in organisations. **European Journal of Information Systems**, v. 18, n. 2, p. 106-125, 2009. Disponível em: https://www.tandfonline.com/doi/full/10.1057/ejis.2009.6 . Acesso em: 26 de abr. 2022.

HÖNE, K.; ELOFF, J. H. P. What makes an effective information security policy?. **Network Security**, v. 2002, n. 6, p. 14-16, 2002. Disponível em: https://www.sciencedirect.com/science/article/pii/S1353485802060117 . Acesso em: 2 ago. 2022.

HWANG, Inho et al. Security awareness: The first step in information security compliance behavior. **Journal of Computer Information Systems**, v. 61, n. 4, p. 345-356, 2021. Disponível em: https://doi.org/10.1080/08874417.2019.1650676 . Acesso em: 21 abr. 2022.

JALALI, M. S.; SIEGEL, M.; MADNICK, S. Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. **The Journal of Strategic Information Systems**, v. 28, n. 1, p. 66-82, 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S0963868717304353?via%3Dihub . Acesso em: 21 abr. 2022.

JEAN-PIERRE, J. J. User Awareness and Knowledge of Cybersecurity and the Impact of training in the Commonwealth of Dominica. 2021. Tese de Doutorado. **Walden University**. Disponível em: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11861&context=dissertations . Acesso em: 12 abr. 2022.

KAHOOT! ASA; What is Kahoot!? , 2019 Disponível em: https://kahoot.com/what-is-kahoot/ Acesso em: 2 ago. 2022.

KAPP, K. M.; FARDO, M. L. The gamification of learning and instruction: game-based methods and strategies for training and education. San Francisco: Pfeiffer, 2012. CONJECTURA: filosofia e educação, v. 18, n. 1, p. 201-206, 2013. Disponível em: https://www.amazon.com.br/dp/B007XA3ME6/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1 . Acesso em: 6 abr. 2022.

KRATH, J.; SCHÜRMANN, L.; VON KORFLESCH, H. F. O. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. **Computers in Human Behavior**, v. 125, p. 106963, 2021. Disponível em:

https://www.sciencedirect.com/science/article/pii/S0747563221002867 Acesso em: 10 ago. 2022.

MAJURI, J.; KOIVISTO, J.; HAMARI, J. Gamification of education and learning: A review of empirical literature. In: Proceedings of the 2nd international GamiFIN conference, **GamiFIN** 2018. CEUR-WS, 2018. Disponível em: https://trepo.tuni.fi/bitstream/handle/10024/104598/gamification_of_education_2018.pdf Acesso em: 10 ago. 2022.

MATIFIC - EDUCATIONAL MATHS GAMES; Pedagogia da Matific, 2022; Disponível em: https://www.matific.com/bra/pt-br/home/pedagogy/principles/ Acesso em: 2 ago. 2022.

MCCROHAN, K. F.; ENGEL, K.; HARVEY, J. W. Influence of awareness and training on cyber security. Journal of internet Commerce, v. 9, n. 1, p. 23-41, 2010. Disponível em: http://dx.doi.org/10.1080/15332861.2010.487415 . Acesso em: 26 de abril.

MORE, Josh. Measuring Psychological Variables Of Control In Information Security. Information Security. **SANS**, 2011. Disponível em: https://www.sans.org/white-papers/33594/ . Acesso em: 14 abr. 2022.

PELTIER, T. R. Implementing an information security awareness program. **Inf. Secur. J. A Glob. Perspect**., v. 14, n. 2, p. 37-49, 2005. Disponível em: https://www.tandfonline.com/doi/pdf/10.1201/1086/45241.14.2.20050501/88292.6 . Acesso em: 2 ago. 2022.

RHEE, H.-S.; RYU, Young U.; KIM, C.-T. Unrealistic optimism on information security management. **Computers & Security**, v. 31, n. 2, p. 221-232, 2012. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404811001441?via%3Dihub . Acesso em: 21 abr. 2022.

RICHARDSON, P. J., et al., Pesquisa Social; Métodos e Técnicas, 3ª Edição, Atlas, São Paulo, 1999. Disponível em : https://climatechangemoz.com/wp-content/uploads/2020/04/Metodologia-de-Pesquisa-Social-Richardson.pdf. Acesso em: 07 nov. 2022

ROGERS, E. M. Diffusion of innovations. Simon and Schuster, 2010. Disponível em: https://teddykw2.files.wordpress.com/2012/07/everett-m-rogers-diffusion-of-innovations.pdf . Acesso em: 21 abr. 2022.

SAS, M. et al. NIST Special Publication 800-16. Information Technology Security Training Requirements: A Role-and Performance-Based Model. Gaithersburg, **MD: US Department of Commerce**, p. 800-16, 1998. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-16/final . Acesso em: 21 abr. 2022.

SAS, Marlies et al. The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. **Safety science**, v. 144, p. 105447, 2021. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0925753521002915 . Acesso em:

26 de abr. 2022.

SHAW, Ruey Shiang et al. The impact of information richness on information security awareness training effectiveness. **Computers & Education**, v. 52, n. 1, p. 92-100, 2009. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0360131508001012 . Acesso em: 6 abr. 2022.

WILSON, M.; HASH, J. SP 800-50. Building an Information Technology Security Awareness and Training Program. National Institute of Standards & Technology, Gaithersburg, **MD: US Department of Commerce** v. 800, n. 50, p. 1-39, 2003. https://csrc.nist.gov/publications/detail/sp/800-50/final . Acesso em: 18 abr. 2022.

ZICHERMANN, G.; CUNNINGHAM, C. Gamification by design: Implementing game mechanics in web and mobile apps. " **O'Reilly Media, Inc**.", 2011. Disponível em: https://books.google.com.br/books/about/Gamification_by_Design.html?id=Hw9X1miVMMwC&redir_esc=y . Acesso em: 28 abr. 2022.

ZWILLING, Moti et al. Cyber security awareness, knowledge and behavior: A comparative study. **Journal of Computer Information Systems**, v. 62, n. 1, p. 82-97, 2022. Disponível em: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1712269 . Acesso em: 6 maio. 2022.

Agradecimentos

Gostaria de agradecer a todos que me ajudaram no desenvolvimento deste trabalho e aos amigos e familiares que me deram todo o apoio que necessitava. Agradeço aos meus pais Carmen Maria Andreazza e Eraldo Pereira Marinho pelas sugestões que foram essenciais ao desenvolvimento deste trabalho.

Agradeço especialmente ao coordenador do curso de Segurança da Informação da Fatec de Americana, Rogério Nunes de Freitas, e aos demais coordenadores pela ajuda com a divulgação dos questionários. Agradeço aos alunos Lara Vitoria Silva Scaramuzza, Luiz Felipe Panini dos Santos, Clara Sass Mariano, Maicon Rodrigo Evangelista, Vitor Barboza Batista, e aos demais alunos que ajudaram a divulgar e participaram da pesquisa. Agradeço também a Beatriz Maria Nunes Pinto e Brito pela sua valiosíssima ajuda com o design da cartilha e divulgação da mesma.

Por último, agradeço o meu orientador Jonas Bodê por toda sua atenção e disponibilidade para comigo e o desenvolvimento deste trabalho.