UNIVERSIDADE ESTÁCIO DE SÁ

Rodrigo Tavares Sozza

GAMIFICAÇÃO COMO TÉCNICA DE CONSCIENTIZAÇÃO DE SEGURANÇA

Uma breve análise sobre a abordagem gamificada no engajamento sobre o tema segurança da informação

SÃO PAULO,

2020.

UNIVERSIDADE ESTÁCIO DE SÁ

Rodrigo Tavares Sozza

GAMIFICAÇÃO COMO TÉCNICA DE CONSCIENTIZAÇÃO DE SEGURANÇA

Uma breve análise sobre a abordagem gamificada no engajamento sobre o tema segurança da informação

Trabalho Científico apresentado à Universidade Estácio de Sá, como requisito final para obtenção do Diploma de Pós-Graduação em Segurança da Informação.

Profª. Orientadora: Adriana de Souza Carvalho.

SÃO PAULO,
2020.

RESUMO

O artigo percorre os princípios de segurança da informação, buscando a necessidade e propósito da conscientização de segurança, discorrendo sobre os principais desafios com relação ao fator humano, protagonista do contexto de conscientização de segurança, ameaças inerentes à sua interface com os ativos de informação e também dos desafios na transformação de comportamento para um uso responsável e consciente, aliado às boas práticas de segurança. O artigo evidencia a necessidade de se trazer engajamento ao processo de conscientização e propõe uma abordagem explorando a gamificação como método de potencial eficiência para esta finalidade.

Palavras-Chaves: Gamificação. Segurança. Informação. Conscientização.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia cada dia mais expande as possibilidades de comunicação entre as pessoas, gerando novas interfaces, fontes de dados e ativos de informação. Frente a esta realidade, os riscos de segurança da informação e as iniciativas correspondentes para sua mitigação também crescem de forma perpendicular, gerando um cenário onde os esforços para um uso responsável e consciente dos recursos tecnológicos são imprescindíveis.

Este uso consciente está muito alinhado com o conhecimento das ameaças e como evitá-las, ou ainda, reduzir seu grau de risco, o que só é possibilitado através de educação voltada ao tema; esta frente é reconhecida por programa de conscientização de segurança da informação.

O principal foco de um programa de conscientização, é preparar as pessoas, transformando seu comportamento, para que evitem incidentes de segurança ou que respondam à eles de modo a reduzir seu impacto, diminuindo assim o risco. No entanto, é notório que a abordagem tradicional de implantação de um programa resumido em um canal para divulgação de conteúdo de boas práticas e a adoção de uma Política de Segurança da Informação não se mostram suficientemente eficazes, em constatação a grande incidência de casos de falha de segurança de origem interna e o fator humano sendo continuamente relacionado como o elo mais fraco.

A adoção de estratégias gamificadas, utilizando elementos de jogos para a educação em segurança, traz novos componentes de interatividade e engajamento, potencializando a motivação para a educação no tema e podendo ser um recurso estratégico a ser utilizado para alcançar um maior número de pessoas em um programa de conscientização de segurança.

O presente trabalho visa reunir e analisar sob uma ótica qualitativa, os princípios chave de segurança, explorar os riscos e requisitos inerentes ao fator humano sob a perspectiva de segurança da informação e abordar a gamificação como fonte de engajamento.

Este trabalho foi realizado através de levantamento bibliográfico, utilizando metodologia bibliográfica e parcialmente exploratória, apenas para que fosse possível traçar linearidade entre os desafios requeridos pela conscientização em segurança e os benefícios ofertados pela gamificação. Foram utilizados livros especializados sobre o tema e também artigos acadêmicos consultados na internet, frutos de pesquisa.

2 CONSCIENTIZAÇÃO DE SEGURANÇA

A segurança da informação têm como base três princípios: confidencialidade, integridade e disponibilidade. Ainda que a estratégia para a garantia destes princípios possa variar, são eles que norteiam as iniciativas voltadas à segurança da informação. Campos (2007, p. 17) afirma que “Se um ou mais desses princípios forem desrespeitados em algum momento, isto significa uma quebra de segurança da informação”. O evento oriundo da quebra de segurança da informação ou exploração de uma vulnerabilidade é considerado um incidente.

A estratégia de implantação de segurança da informação objetiva estabelecer os critérios adequados, considerando os três princípios mencionados, de forma responsável, com foco em pessoas, processos e tecnologias; no entanto, é perceptível uma atenção desproporcional entre os três fatores, dos quais, tecnologia acaba geralmente sendo o maior alvo de esforços e investimentos.

Segundo Russel (2002, p. 3, tradução nossa):

> Enquanto confidencialidade, integridade e disponibilidade representam quais aspectos de informação e ativos de informação estão sendo protegidos; pessoas, processos e tecnologia descrevem como essa proteção ocorre. Todos três fatores de pessoas, processos e tecnologia exercem um papel igualmente importante na segurança da informação. Entretanto, controles técnicos, como firewalls, frequentemente recebem toda atenção e pessoas e processos são negligenciados.

A falta de investimentos adequados para a educação e conscientização é um dos grandes empecilhos para a segurança da informação. Para Gardner e Thomas (2014, p. 2, tradução nossa):

> Por anos, organizações têm despejado dinheiro em segurança, quando este dinheiro poderia ser melhor gasto treinando seus usuários.

Esta relação de investimentos desproporcionais demonstra que, apesar do alto risco envolvendo o fator humano, este é comumente subestimado e despriorizando entre as ações de combate às ameaças de cibersegurança.

A Tecnologia da Informação, tendo as pessoas como princípio e fim, deve considerá-las em todas etapas e, sob a ótica de Segurança da Informação, um projeto ou iniciativa, só pode ser bem sucedido, quando este fator humano é levado em conta de forma apropriada, considerando todo o seu ciclo de vida de interações, seja com ativos de informação ou com as demais pessoas, no contexto dos princípios anteriormente mencionados (confidencialidade, integridade disponibilidade).

Este cuidado é necessário para que seja possível a adoção de uma postura responsável com relação ao risco, já que, o fator humano é frequentemente apontado como sendo o elo mais fraco, ou o ponto de falha mais comum sob a perspectiva de segurança da informação, conforme sugere Mitnick (2003, p. 1, tradução nossa):

> Companhias estão mais conscientes do que nunca sobre segurança, dedicando atenção sobre tecnologias sofisticadas e defesas físicas para proteger seu capital intelectual. Mas eles têm negligenciado o elo mais fraco: seus empregados. São estes trabalhadores da linha de frente e de nível médio que estão crescentemente sendo alvos de intrusos e que involuntariamente entregarão as chaves do reino.

As pessoas, que utilizam no seu cotidiano diversos dispositivos eletrônicos (notebooks e celulares, por exemplo), credenciais de acesso - tanto físico (exemplos: crachá, cartão de acesso) como lógico (exemplos: login, token), além de acesso à diversos ativos de informação (computadores e até documentos físicos, como contratos) podem ser alvos de ataques e, passivamente, gerarem incidentes de segurança, mas também, estas pessoas podem ser os causadores intencionais dos incidentes de segurança da informação. Para Gardner e Thomas (2014, p. 1, tradução nossa):

> Em segurança da informação, as pessoas são o elo mais fraco. Pessoas querem ser prestativas. Pessoas querem realizar um bom trabalho. Pessoas querem proporcionar um bom atendimento para seus colegas de trabalho, clientes e fornecedores. Pessoas são curiosas.

Considerando um ecossistema entre pessoas e sua relação com os ativos de informação, a conscientização de segurança se faz necessária para uma utilização responsável, reduzindo o risco de segurança, de modo a transformar seu comportamento para um uso e interação consciente e aceitável sob os critérios e boas práticas de segurança. Para Wilson e Hash (2003, p. 7, tradução nossa):

> Um programa de conscientização e treinamento é crucial pois é o veículo de disseminação de informação que usuários, incluindo gerentes, precisam para realizar seus trabalhos. No caso de um programa de segurança de TI, é um veículo para ser usado para comunicar requisitos de segurança por toda empresa.

Um programa bem sucedido de conscientização de segurança é aquele que capacita as pessoas que tenham compreensão de sua responsabilidade com a segurança da informação, para que sejam capazes de detectar possíveis ameaças e que também possam responder a elas de maneira adequada, reduzindo ou mitigando os riscos de segurança; é capaz de influenciar o comportamento positivamente, para que as pessoas entendam os riscos e assim decidam realizar melhores escolhas e estejam mais conscientes de suas ações e responsabilidades com relação as potenciais ameaças.

Para Russel (2002, p. 4, tradução nossa):

> O objetivo primário de um programa de conscientização de segurança é educar usuários sobre sua responsabilidade em proteger a confidencialidade, disponibilidade e integridade da informação e ativos de informação de sua organização. Segurança da Informação é responsabilidade de todos, não apenas do departamento de TI. É crítico que os usuários entendam não apenas como proteger a informação da organização, mas porque é importante proteger aquela informação.

Objetivamente, a educação das pessoas incide diretamente em sua capacidade de agir de forma mais segura. Encontrar meios efetivos de conscientização deve ser uma prioridade para um programa bem sucedido de segurança da informação.

2.1 Engajamento

Um dos desafios inerentes à etapa de conscientização de segurança, é o engajamento das pessoas com relação ao programa. Criação de material e comunicação que não alcança as pessoas, além de dispendioso, é ineficaz.

Os esforços direcionados à Segurança da Informação são constantes e permanentes, já que, a contrapartida das vulnerabilidades e ameaças também o são, sendo assim, é natural que um programa de conscientização também seja contínuo, abordando novas tendências - ou seja, é também importante que, como ativos de segurança, as pessoas também sejam constantemente atualizadas. Esta educação exige tempo, esforço e geralmente concorre com outras atividades e metas nas organizações, além do conteúdo muitas vezes estar desconectado da realidade dos colaboradores ou não usar uma comunicação, linguagem ou metodologia adequada. Garantir o engajamento das pessoas para tal efeito consiste em um desafio. Voss (2001, p. 3, tradução nossa) acrescenta:

> Para a maioria da população corporativa em geral, o assunto segurança pode ser bastante chato. Também pode instilar sentimentos de medo e frustração por causa da ideia que segurança na companhia somente atrapalha um trabalho bem feito".

É importantíssima a aplicação de linguagem adequada, própria ao público a qual se destina, para que seja possível uma conexão com sua audiência, tornando mais eficaz a propagação da mensagem de segurança da informação. Há uma grande escassez de práticas que envolvam o público, criem novas dinâmicas e que gerem o engajamento necessário.

Segundo um estudo do SANS (2017, p. 9), comunicação e engajamento estão, respectivamente, entre os maiores desafios com relação a conscientização de segurança da informação.

Figura 1 - Maiores desafios na conscientização de segurança

Major Challenges	Responses	%
Communication	113	15.98%
Employee Engagement	101	14.29%
Time	95	13.44%
Culture	85	12.02%
Resources	83	11.74%
Upper Management Support	80	11.32%
Other	66	9.34%
Money	42	5.94%
Enforceability of Program	31	4.38%
Staff	11	1.56%
Total	707	100%

Fonte: SANS Security Awareness Report (2017)

Para Hughes (2020, n.p., tradução nossa):

> Especialistas concordam que o treinamento tradicional de segurança não funciona e que funcionários destreinados são o maior risco para o negócio. A gamificação do seu programa de conscientização pode ajudar você a criar uma oportunidade de aperfeiçoar sua equipe e também ajudá-los a se defender e sua companhia de ciberameaças.

Grande parte das organizações possuem um programa de conscientização de segurança, mas mesmo assim, enfrentam dificuldades por não conseguir obter os resultados esperados com o programa. As ações preventivas, como um programa eficaz de conscientização, poderia salvar custos que são feitos nas etapas de remediação dos incidentes. Os esforços na fase preventiva são oportunos, já que nas fases seguintes do ciclo de vida de um incidente podem ser tardios e tempo, em uma perspectiva de resposta a incidentes, é algo crítico e vital.

2.2 Gamificação

A gamificação (ou ainda, ludificação), oferece recursos interessantes para trazer um conteúdo interativo, podendo ser uma nova forma de alcançar as pessoas e trazer maior engajamento ao tema segurança da informação. Vianna *et al*. (2013, p. 10), define “A gamificação (do original em inglês gamification) corresponde ao uso de mecanismos de jogos orientados ao objetivo de resolver problemas práticos ou de despertar engajamento entre um público específico.”

O engajamento é necessário para um melhor aproveitamento do conteúdo, o uso de técnicas gamificadas na educação é uma abordagem que potencializa o ensino, tornando-o mais eficaz. Segundo Alves (2015, p. 14):

> O que funcionava antes não necessariamente funciona hoje quando o assunto é aprendizagem. É neste cenário que o Gamification se encaixa. Ajudando-nos a tornar a aprendizagem atrativa, engajadora, divertida e efetiva.

A conscientização tradicional, muitas vezes, aborda questões desconectadas da realidade das pessoas, adicionalmente, servem um propósito de conformidade mas sem apresentar resultados efetivos com relação à redução de risco. Para Hughes (2020, n.p., tradução nossa):

> Toda organização tem a tarefa de aumentar a conscientização sobre segurança cibernética e mudar os comportamentos de segurança do usuário. Endereçar esse desafio requer o engajamento de todos os funcionários, independentemente do nível de habilidade por meio de conteúdo dinâmico, eficaz e envolvente. Mas isso requer mais do que apresentações em PowerPoint e cursos anuais obrigatórios que nada mais são do que um exercício regulatório de checagem.

De forma divertida e engajadora, a gamificação já têm sido utilizada para educação e também para reforçar comportamento nas organizações, alinhada com a segurança da informação, pode trazer resultados positivos na conscientização e mudança de comportamento. Para Vianna *et al*. (2013, p. 10):

> Com frequência cada vez maior, esse conjunto de técnicas tem sido aplicado por empresas e entidades de diversos segmentos como alternativas às abordagens tradicionais, sobretudo no que se refere a

> encorajar pessoas a adotarem determinados comportamentos, a familiarizarem-se com novas tecnologias, a agilizar seus processos de aprendizado ou de treinamento e a tornar mais agradáveis tarefas consideradas tediosas ou repetitivas.

Uma das principais vantagens das abordagens gamificadas certamente é o engajamento. A diversidade de temas, dinâmicas e diversão podem potencializar resultados positivos para a educação. Segundo Alves (2015, p. 15):

> Outro fato que não podemos ignorar é o poder que os games exercem sobre as pessoas. Muitos de nós já experimentaram a sensação de jogar por horas sem percebermos o tempo passar. Compreender o que há nos jogos e os elementos envolvidos para se promover este engajamento pode nos ajudar a transportar este engajamento para o ambiente de aprendizagem.

É possível aplicar a gamificação nas práticas de conscientização e educação de segurança da informação. Vianna *et al*. (2013, p. 23) afirma que “Sem dúvida, um dos principais fatores que justificam todo o interesse que os jogos têm despertado ultimamente se deve à percepção da atratividade que eles exercem sobre nós, e de como essa capacidade de gerar engajamento e dedicação pode ser aplicada a outros propósitos como, por exemplo, o contexto corporativo”.

Para Hughes (2020, n.p., tradução nossa):

> Estratégias de segurança necessitam unir departamentos e abordá-los com uma mentalidade de fora dos times de segurança de TI para obter engajamento do negócio. Para transformar seu treinamento de cibersegurança, você precisa trazer todos os funcionários e todos os aspectos do seu negócio juntos para o passeio. A melhor forma de finalmente alinhar gestão de risco e cibersegurança é fazê-la de forma divertida, engajadora e competitiva para todos.

3 CONSIDERAÇÕES FINAIS

Como pode ser apresentado neste artigo, as pessoas são essenciais para a segurança da informação. Não é possível endereçar risco sem levar em consideração o fator humano, este ainda, é negligenciado pelas companhias, que não enxergam o valor em sua educação e continuam sendo o elo mais fraco na tríade pessoas, processos e tecnologia. Direcionar esforços para a conscientização e educação destas pessoas pode resultar em um cenário em que, ao invés de elo mais fraco, elas poderão se posicionar como responsáveis pela segurança da informação em suas atividades, agindo de forma consciente e ajudando na prevenção de incidentes.

Uma abordagem tradicional, apenas considerando a adoção de uma política de segurança da informação e uma mínima comunicação, pode se mostrar ineficaz, pois as pessoas necessitam de diferentes abordagens, utilizando diferentes canais e precisam estar e se manter engajadas sobre o tema segurança, garantir este engajamento é um grande desafio, já que as pessoas podem não enxergar valor direto nas ações de segurança. Uma nova abordagem, trazendo os recursos de gamificação podem trazer maior engajamento e uma forma divertida para se tocar no assunto segurança da informação, alcançando mais pessoas e aproximando-as da missão de tornar o ambiente organizacional mais seguro.

REFERÊNCIAS

CAMPOS, André. **Sistema de Segurança da Informação**: Controlando os Riscos. 2. ed. Florianópolis: Visual Books, 2007.

RUSSEL, Chelsea. **Security Awareness** - Implementing an Effective Strategy. Disponível em: <https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418>. Acesso em: 22 Abr. 2020.

MITNICK, Kevin. **Are you the weak link**. Disponível em: <https://hbr.org/2003/04/are-you-the-weak-link>. Acesso em: 22 Abr. 2020.

GARDNER, Bill; THOMAS, Valerie. **Building an Information Security Awareness Program**: Defending Against Social Engineering and Technical Threats 1st Edition. Disponível em: <https://www.researchgate.net/publication/291092430_Building_an_Information_Security_Awareness_Program_Defending_Against_Social_Engineering_and_Technical_Threats_1st_Edition>. Acesso em: 22 Abr. 2020.

WILSON, Mark; HASH, Joan. **Building an Information Technology Security Awaraness and Training Program**. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf>. Acesso em: 22 Abr. 2020.

VOSS, Brian. **The Ultimate Defense of Depth**: Security Awareness inYour Company. Disponível em: <https://www.sans.org/reading-room/whitepapers/awareness/ultimate-defense-depth-security-awareness-company-395>. Acesso em: 22 Abr. 2020.

SANS. **Security Awareness Report**. Disponível em: <https://www.sans.org/sites/default/files/2017-12/STH-SecurityAwarenessReport-2017.pdf> Acesso em: 22 Abr. 2020.

HUGHES, Neil C. **How gamification can transform cybersecurity training**. Disponível em: <https://cybernews.com/security/how-gamification-can-transform-cybersecurity-training/> Acesso em: 22 Abr. 2020.

ALVES, Flora. **Gamification** : como criar experiências de aprendizagem engajadoras: um guia completo do conceito. 2. ed. São Paulo: DVS Editora, 2015.

VIANNA, Y; VIANNA, M; MEDINA, B; TANAKA, S. **Gamification, Inc**: como reinventar empresas a partir de jogos. 1. ed. Rio de Janeiro: MJV, 2013.