Q.U.A.S.E.: uma metodologia ágil para diagnóstico de ataques de *phishing*

Helton Garcia[1], Rafael Rabelo Nunes[2], João Souza Neto[2]

[1] Tribunal de Contas da União (TCU), SAFS Q4, LT 1, CEP 70042-900 Brasília-DF

[2] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF

heltongarcia@gmail.com {rafaelrabelo,neto.joão}@unb.br

Abstract. *This article presents the Q.U.A.S.E. methodology, developed to facilitate the identification of signs of phishing in e-mails by end users. It is based on just five elements, allowing a quick assessment of suspected messages. The methodology aims to be easy to apply and has low training costs. The proposal has been practiced since the first half of 2022 in internal training at Brazilian Federal Court of Accounts (TCU) . The results obtained in annual classes have demonstrated the effectiveness in achieving results from phishing attack simulations as part of an ongoing user education program.*

Resumo. *O presente artigo apresenta a metodologia Q.U.A.S.E., desenvolvida para facilitar a identificação de indícios de phishing em e-mails por parte de usuários finais. Fundamenta-se em cinco elementos, permitindo uma rápida avaliação de conteúdo suspeito. A metodologia se propõe ser de fácil aplicação e baixo custo de treinamento. A proposta tem sido praticada desde o primeiro semestre de 2022 em treinamentos internos no Tribunal de Contas da União (TCU). Os resultados obtidos em turmas anuais demonstraram a eficácia no alcance de resultados de simulações de ataques de phishing como parte de programa continuado de educação de usuários.*

1. Introdução

A transformação digital representa salto significativo na maneira como organizações executam seus negócios. Nesse sentido, novas tecnologias são adotadas, bem como as já consolidadas, como mensagens eletrônicas (e-mails). O relatório publicado pela The *Radicati* Group intitulado *Email Statistics Report, 2021-2025* [Radicati 2024] estima que até 2025 o total de e-mails circulantes na internet chegue a 376 bilhões por dia. O e-mail tornou-se uma ferramenta de trabalho indispensável devido à sua eficiência, rapidez e versatilidade na comunicação.

O mundo corporativo depende de tecnologias como e-mail. Por outro lado, a dependência digital traz consigo a possibilidade de ocorrência de vulnerabilidades em sistemas e soluções, capazes de serem exploradas por atacantes, gerando potenciais consequências.

O relatório anual *Cyber Security Breaches Survey* publica pesquisas sobre violações de segurança cibernética no Reino Unido. O estudo explora as políticas, processos e abordagem para segurança cibernética, para empresas, instituições de

caridade e instituições educacionais. Nas últimas edições, de 2021 a 2024, *phishing* permanece como, nos termos dos relatórios, “de longe" o tipo mais comum de ataque, com tendência de aumento percentual entre as edições no setor corporativo [Ell 2024; Johns 2023].

Nesse ambiente de ameaças foi desenvolvida uma metodologia própria, denominada Q.U.A.S.E., que objetiva conscientizar usuários finais na identificação rápida e prática de mensagens contendo *phishing*. A proposta foi concebida para oferecer simplicidade ao usuário, para que possa ser realmente adotada para identificar mensagens suspeitas com apenas cinco passos, dentro de relação custo-benefício, o que se diferencia de outras abordagens, como a publicação *NIST Phish Scale User Guide* [Dawkins and Jacobs 2023].

O Q.U.A.S.E. foi proposto inicialmente no primeiro semestre de 2022 e vem sendo empregado e aprimorado em treinamentos de conscientização de usuários em segurança cibernética no TCU, contribuindo para a mitigação de riscos associados a ataques capazes de explorar fragilidades humanas. A experiência sedimentada com o tempo evidencia a abordagem prática e a originalidade, sobretudo quando comparada a outras metodologias lançadas posteriormente e mais complexas. O *feedback* dos alunos contribuiu para a simplificação da proposta ao longo das versões.

O cenário de ataques cibernéticos cada vez mais frequentes demanda o uso de instrumentos ágeis e práticos para que os usuários não sejam impactados significativamente em suas rotinas para que possam incorporar novos pequenos hábitos e, assim, mitigar riscos de clicarem em links maliciosos e serem capazes de identificar conteúdos suspeitos relacionados a *phishing*.

O impacto de ser vitimado por um clique indevido pode ser grande. Desde o comprometimento da própria conta associada ao usuário até mesmo da rede corporativa, pelo escalonamento de privilégios e outras técnicas adotadas pelo atacante.

Então, os impactos decorrentes são significativos e ações de conscientização e educação de usuários tornam-se necessária para garantir que boas práticas fundamentais de segurança cibernética sejam internalizadas e reforçadas periodicamente, como parte integrante de medidas de *cyber higiene* voltadas ao usuário final. Nesse sentido, a implementação de medidas preventivas torna-se imprescindível para a proteção de ativos digitais da organização.

O presente trabalho tem como objetivo apresentar a metodologia Q.U.A.S.E., voltada para usuários finais identificarem e-mails suspeitos de forma simples e ágil, para que possa concentrar-se em suas atividades ordinárias.

Em uma analogia didática, como seria adotar um guarda-chuva que fosse pouco prático de ser manuseado e difícil de ser transportado. Mesmo em dias de previsão meteorológica ruim, seria viável sair de casa com ele ou seria melhor aceitar o risco de se molhar? O Q.U.A.S.E. se propõe a ser um guarda-chuva portátil e de fácil manuseio.

2. Referencial teórico

Nessa seção, apresentam-se os conceitos necessários para que se compreenda esse trabalho. Primeiro, discorre-se sobre *phishing* como veículo de entrada para um ataque. Em seguida, tipos de *phishing*, bem como sua relação com o envio de artefatos maliciosos.

Também são apresentados fatores comportamentais e tecnológicos relacionados ao tema. Por fim, uma breve abordagem sobre impactos.

2.1. *Phishing* como vetor inicial de ataque

Phishing é um dos pontos de entrada mais prevalentes no espaço cibernético, sendo frequentemente apontado como causa inicial de violações de dados [Caridi et all 2024; Mimecast 2024]. O método destaca-se pela sua simplicidade e eficácia, sobretudo ao explorar fragilidades humanas por meio de técnicas de engenharia social, como senso de urgência, promessas de vantagens ou ameaças [Bassett et al. 2022].

Alabdan (2020) analisa diversas variações que miram grupos específicos ou a alta gestão. Lella et al. (2024) apresenta variantes capazes de dificultar a detecção por mecanismos tradicionais. Técnicas como *spoofing* de e-mails são frequentemente utilizadas para simular legitimidade e enganar vítimas. É um dos pilares de fraudes como Business E-mail Compromise, que causaram perdas superiores a US$ 2,9 bi em 2023 [FBI 2023]. Mais recentemente, o malware Pegasus foi lançado, sendo capaz de não requerer interação da vítima [Lella et al. 2024].

A literatura e experiências práticas demonstram que a mitigação de *phishing* não pode depender exclusivamente de soluções tecnológicas. É imprescindível investir em conscientização e treinamentos contínuos, especialmente com modelos simples e aplicáveis como o Q.U.A.S.E., voltado ao usuário final, para fortalecer a resiliência organizacional frente a esse tipo de ameaça [Dawkins and Jacobs 2023].

2.2. Fatores comportamentais, tecnológicos e impactos do *phishing*

Phishing continua sendo amplamente eficaz por explorar o fator humano. Estima-se que 82% das violações envolvem elementos humanos, como erro, uso de credenciais comprometidas e *phishing* [Bassett et al. 2022]. Técnicas psicológicas como *nudges*, botões destacados, linguagem persuasiva ou apelos emocionais, são amplamente empregadas para reduzir o tempo de reação da vítima e aumentar a taxa de sucesso do ataque [Sjouwerman 2024].

Mensagens falsas muitas vezes simulam padrões internos da organização. Pesquisa da KnowBe4 (2024) mostra que modelos visuais familiares e comunicações rotineiras da própria organização são os mais eficazes em enganar vítimas. A coleta prévia de dados via mídias sociais potencializa essa manipulação.

A proteção baseada apenas em ferramentas como antivírus e filtros de e-mail se mostra insuficiente frente a ataques sofisticados [Heimdall, 2021]. O relatório da Microsoft [Terranova 2024] ressalta que a cultura organizacional de segurança, apoiada por treinamento contínuo, é fator-chave para mitigação de riscos. A aplicação do princípio da defesa em profundidade — combinando tecnologia, processos e comportamento — é essencial para resiliência cibernética [AICD 2022].

O impacto de um clique em *phishing* pode ser significativo: roubo de credenciais, vazamento de dados sensíveis, instalação de malware, e comprometimento da rede corporativa. Casos de *ransomware*, frequentemente distribuídos por *phishing*, geram sequestros digitais com exigência de resgate e riscos de exposição de dados [McCabe 2023].

O *phishing* é também lucrativo e de fácil execução, com kits prontos disponíveis online, baixo custo e alta escalabilidade. O FBI (2023) estimou perdas superiores a US$ 2,9 bilhões apenas com fraudes via e-mail. Esse cenário reforça a urgência de programas de treinamento permanentes e adaptados à realidade organizacional. Afinal, como alertam Moura e Oerting (2019), não se trata de *se* haverá um incidente, mas de *quando* ele ocorrerá.

3. Trabalhos correlatos

No decorrer da pesquisa, identificou-se alguns trabalhos relacionados a boas práticas de segurança da informação envolvendo o tema *phishing*, publicados no Brasil e no exterior. A abordagem inicial foi buscar publicações que tivessem abordagem similar ao modelo proposto, simples e de fácil entendimento para o usuário final. Posteriormente à criação da versão inicial do presente modelo, houve a publicação de guias com abordagem similar. Foram desconsiderados no levantamento, modelos exclusivamente baseados em infográficos ou postagens que careciam de apresentação metodológica [CISA-FBI 2024; Dawkins and Jacobs 2023; MS-ISAC 2023].

O documento NIST Phish Scale tem como objetivo classificar a dificuldade de detecção humana de e-mails de *phishing*, por parte de usuários A metodologia é dividida em duas categorias: pistas observáveis (*cues*) e alinhamento da premissa do e-mail com o contexto do destinatário (*premise alignment*). De forma geral, quanto mais pistas, mais fácil seria identificar um e-mail como *phishing* [Dawkins and Jacobs 2023].

O documento intitulado *Update to Phishing General Security Postcard* foi publicado em janeiro de 2024 e se trata de uma cartilha resumida sobre orientações para identificar ataques de *phishing*, bem como explicar como reportar incidentes e mitigar riscos [CISA-FBI 2024].

O documento intitulado *Phishing Guidance: Stopping the Attack Cycle at Phase One* foi publicado em outubro de 2023, pela MS-ISAC (*Multi-State Information Sharing and Analysis Center*), fornece guia detalhado de orientações para fazer frente a ataques de *phishing* [MS-ISAC 2023].

A publicação **NIST SP 800-50**, *Building an Information Technology Security Awareness and Training Program* propõe a implementação de programa de natureza contínua, alinhada à segurança institucional. Diferencia-se por estabelecer visão programática para segurança em recursos humanos, no âmbito organizacional, sob três pilares fundamentais: conscientização de usuários e treinamento de competências gerais ou específicas [Merritt et al. 2024].

4. Metodologia

4.1. Q.U.A.S.E.

A metodologia Q.U.A.S.E. foi desenvolvida com o objetivo de oferecer uma ferramenta prática e de fácil memorização para identificação de mensagens de *phishing* por usuários finais. Trata-se de uma pesquisa aplicada, com abordagem qualitativa e exploratória, iniciada no primeiro semestre de 2022 no âmbito do TCU, como parte de um programa contínuo de capacitação em segurança da informação. Desde então, a metodologia vem

sendo aprimorada com base em feedbacks das turmas treinadas e aplicada em campanhas anuais de conscientização.

O acrônimo Q.U.A.S.E. refere-se a cinco critérios simples que orientam a análise de mensagens eletrônicas potencialmente maliciosas. Cada elemento corresponde a um ponto de atenção (red flag), cuja presença pode indicar, ainda que não de forma conclusiva, a possibilidade de *phishing*. A Figura 1 sintetiza esses elementos.

A aplicação dos cinco critérios deve ser feita de forma conjunta e rápida. Por exemplo, o simples fato de um endereço de e-mail parecer legítimo não elimina o risco: remetentes podem ser forjados. Assim, mesmo que o campo "Quem" pareça confiável, os demais elementos devem ser analisados.

Mensagens de *phishing* comumente apresentam frases como “clique agora”, “urgente” ou “você ganhou um prêmio”, utilizando a emoção como gatilho de decisão. O clique em um link ou abertura de anexo é a ação desejada pelo atacante, e por isso, a análise do critério [U] é essencial. O item [A] reforça esse ponto ao destacar o risco de arquivos suspeitos ou links disfarçados (ex: domain.com.ru ou jogo.exe).

Já a análise de semelhança com a organização [S] considera aspectos como logotipo, linguagem e estrutura de mensagens internas, que podem ser mimetizados para enganar usuários. Ataques mais sofisticados reutilizam modelos reais da organização, dificultando a identificação de fraude — como boletins, alertas de sistema e ofícios internos.

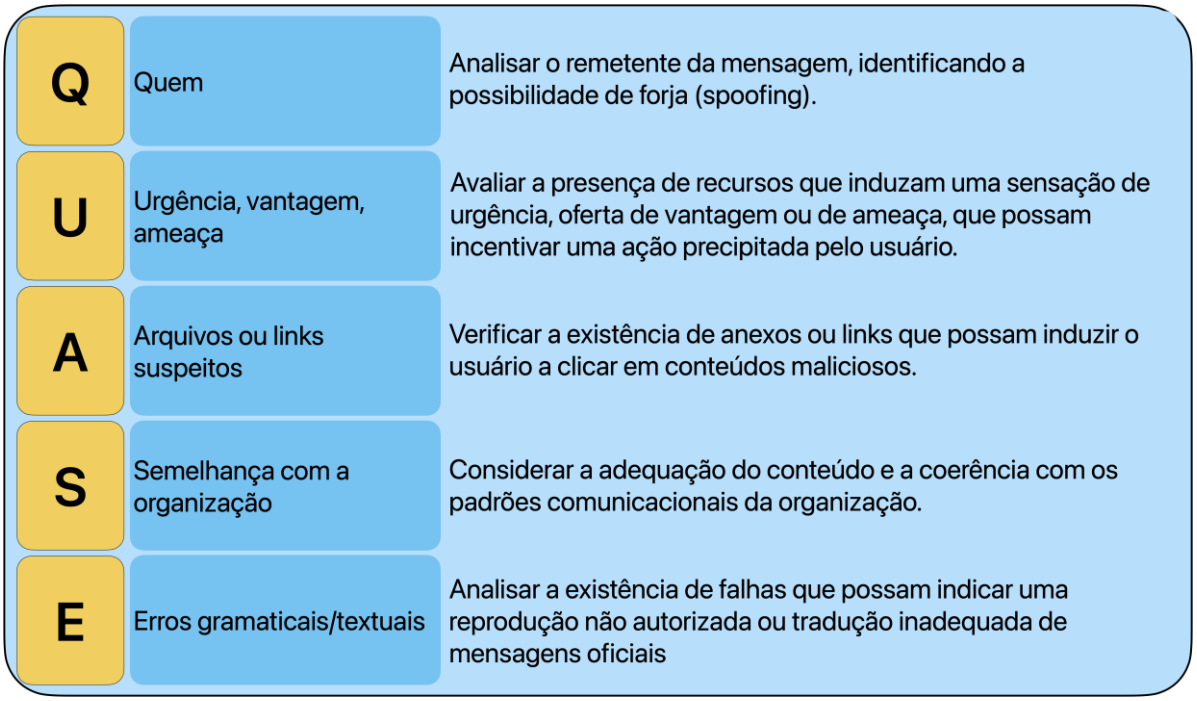

Figura 1 – Metodologia Q.U.A.S.E.

Por fim, erros gramaticais ou de formatação [E], embora mais comuns em ataques genéricos e automatizados, também servem como sinal de alerta. A presença desses elementos pode indicar que a mensagem não foi revisada, ou foi traduzida automaticamente.

Essa estrutura baseada em cinco pontos de atenção foi inspirada em estudos sobre red flags no contexto de segurança da informação e engenharia social, que ainda permanecem adotados, inclusive nos modelos escolhidos para comparação [Herzog 2016]. Seu diferencial está na simplicidade e no foco na experiência do usuário, tornando a metodologia viável para adoção cotidiana, sem sobrecarregar o processamento da caixa de entrada.

4.2. Abordagem

A metodologia Q.U.A.S.E. tem sido utilizada como base para programas de capacitação e sensibilização de usuários em relação a ataques de *phishing*, com enfoque na sua aplicação prática no contexto organizacional. Para isso, adotou-se uma estrutura de avaliação denominada modelo 3T, composta por três etapas sequenciais: Teste inicial (T1), Treinamento (T2) e Teste final (T3), Figura 2. Essa estrutura permite verificar a efetividade da intervenção educativa com base em uma análise comparativa entre os momentos anterior e posterior ao treinamento.

Figura 2 – Estrutura geral da metodologia Q.U.A.S.E. (3T)

A Figura 3 ilustra um exemplo prático da aplicação do modelo 3T, no qual usuários são expostos a campanhas de simulação de *phishing* com características variadas. As dificuldades em escala qualitativa, variam entre fácil, médio e difícil. Cada teste é composto por um conjunto de simulações planejadas e distribuídas ao longo de uma janela temporal esparsa, sem aviso prévio aos participantes, a fim de preservar o fator surpresa e avaliar a prontidão espontânea dos usuários.

A avaliação dos resultados se dá por meio de comparação relativa, e não de valores absolutos. Conforme argumentado por Siadati et al. (2017), a análise baseada em escalas absolutas pode introduzir vieses associados à dificuldade das mensagens, ao conhecimento prévio do público ou à quantidade de indícios presentes nas simulações. Por esse motivo, o escopo metodológico da Q.U.A.S.E. se baseia na diferença entre os desempenhos em T1 e T3: se T3 > T1, considera-se que houve avanço na prontidão dos usuários e, por conseguinte, mitigação do risco cibernético associado ao *phishing*. Resultados inversos indicariam retrocesso ou falhas no processo formativo.

A abordagem acrescenta ainda outras medidas, com vistas a garantir uniformidade mínima de procedimento entre diferentes avaliações e mitigar vieses. a) cada teste é organizado em lotes de simulações, com pelo menos quatro mensagens cada; b) os alunos não recebem aviso prévio, como parte integrante do fator surpresa para o sucesso dos teste; c) o cronograma de realização das simulações (‘janela de teste’) é esparso para que, mesmo após o treinamento, o estado de prontidão volte a ser latente preservando temporalidade sugerida por Siadati et al. (2017); d) as simulações são agendadas em dias aleatórios dentro da janela de teste; e) as dificuldades dos testes são equivalentes, inclusive em relação à pontuação individual das simulações f) nosso público-alvo é bastante heterogêneo e constitui todos os detentores de e-mail contendo o domínio da organização, sendo até 2024, na ordem de 3.600.

Além disso, o ambiente de simulação é configurado para que não sofra interferências das soluções de segurança corporativas. Na fase de planejamento, as simulações são preparadas, testadas e validadas com patrocinadores diretamente envolvidos na iniciativa. O grupo é limitado para garantir que o fator surpresa não seja maculado. Cada simulação contém uma landing page que contém informações importantes para o usuário, a começar pela informação de que se trata de um teste e um breve explicação sobre o que ele poderia ter observado e o que ele poderia fazer para evitar ser vítima novamente.

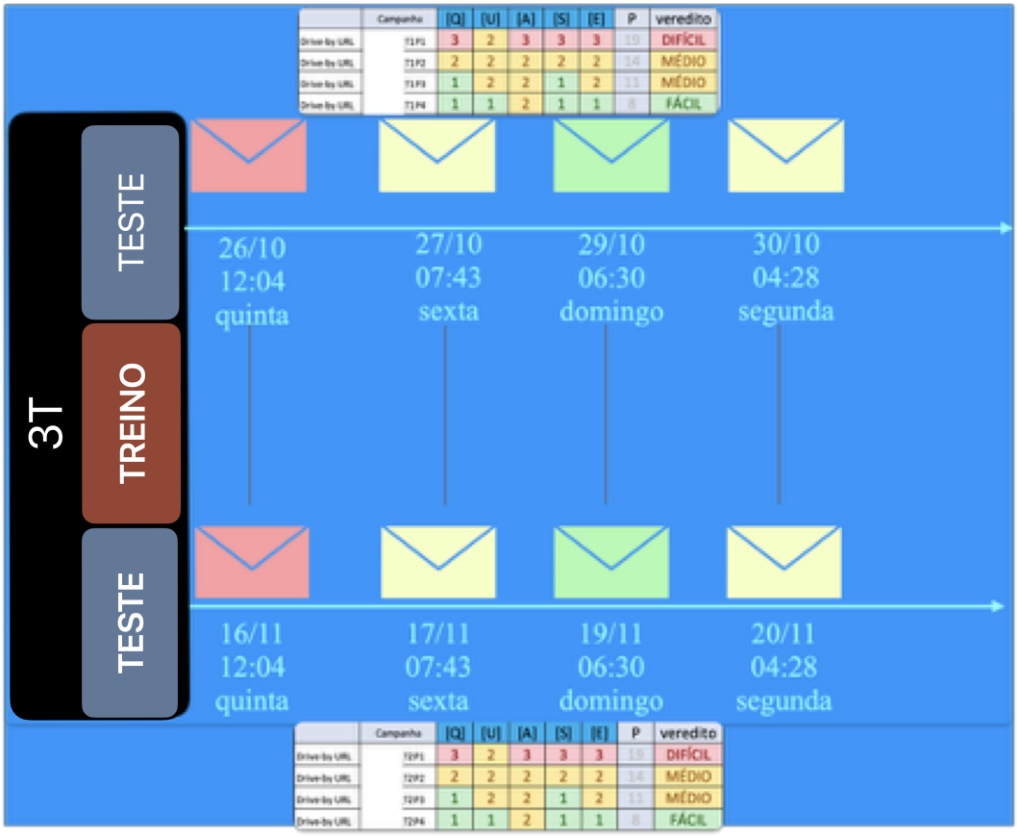

Figura 3 - Exemplo prático de aplicação da metodologia Q.U.A.S.E.

A escala de dificuldade das mensagens é convencionada em pontos, conforme Figura 4. Em geral, quanto mais desafiador é o critério, maior é a pontuação. Então, para o critério de remetente (Q), um contato estranho possui pontuação mínima e um forjado, máxima. Para a semelhança com informações da organização (S), quanto menos familiar, menor a pontuação e vice-versa, para conteúdo mais familiar. E para as demais (U./A./E.) quanto maior a prevalência de elementos, menor a pontuação. E quanto mais discreto for o conteúdo, maior a pontuação.

A pontuação das simulações é realizada considerando a necessidade de realizar várias simulações de em um mesmo teste e com dificuldades diferentes. Foi adotada escala de três pontos para cada critério, cuja fórmula é:

$$T = \sum_{t=1}^{2}(-1)^t * \sum_{s=1}^{S}\left(\left(\frac{F_s}{R_s} * 100\right) * \left(\frac{1}{PA_s}\right)\right);$$

$$\text{onde: } PA_s = \left(\frac{\frac{1}{P}}{\min(\frac{1}{P})}\right) - K; P = \sum_{c=1}^{C}(v_c * p_c),$$

onde T é o valor comparativo final; t é o t-ésimo teste de *phishing*; S é o total de simulações dentro de um teste de *phishing* t; s é a s-ésima simulação dentro de teste de *phishing* t; F é o quantitativo de falhas (*click bait*) dentro de uma simulação s; R é o universo de respondentes de uma simulação s; PA é a pontuação ajustada por dificuldade de uma simulação i; P é a pontuação de uma simulação s; v é o valor obtido de um critério c; p é o peso de um critério c; K é o coeficiente experimental de ajuste da curva de pesos ponderados.

CRITÉRIOS (C)

	v_c	p_c	c
(Q)uem			
O remetente é grosseiramente estranho	1	1	1
O remetente tenta se passar por domínio externo (spoofing ou forja)	2	1	2
O remetente tenta se passar por domínio interno (spoofing ou forja)	3	1	3
(U)rgência/vantagem/ameaça			
O conteúdo muito apelativo sobre urgência, vantagem, ameaça	1	2	2
O conteúdo pouco apelativo sobre urgência, vantagem ou ameaça	2	2	4
O conteúdo é discreto sobre urgência, vantagem ou ameaça	3	2	6
(A)rquivos ou links suspeitos			
Arquivos ou links de fácil associação semântica	1	1	1
Arquivos ou links de associação semântica pouco intuitiva	2	1	2
Arquivos ou links de associação semântica de difícil intuição	3	1	3
(E)rros gramaticais/contextuais			
Erros gramaticais ou contextuais bastante grosseiros ou frequentes	1	1	1
Erros gramaticais ou contextuais menos grosseiros ou pouco frequentes	2	1	2
Erros gramaticais ou contextuais ausentes ou muito poucos	3	1	3
(S)emelhança com organização			
Semelhança completamente alheia à organização	1	2	2
Semelhança pode estar associada à semântica de documentos da organização	2	2	4
O modelo é facilmente confundido com material interno (mimetismo)	3	2	6

PONTUAÇÃO POR SIMULAÇÃO (s)

[Q]	[U]	[A]	[S]	[E]	P	EQ
1	1	1	1	1	7	FÁCIL
...	...	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
1	1	1	2	2	10	FÁCIL
1	2	1	2	1	11	MÉDIO
1	2	1	2	2	12	MÉDIO
...	...	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
2	2	2	2	2	14	MÉDIO
2	2	2	2	3	15	MÉDIO
2	2	3	2	3	16	DIFÍCIL
3	2	3	2	3	17	DIFÍCIL
...	...	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
3	3	3	3	3	21	DIFÍCIL

Figura 4 - Critérios e pontuação da metodologia Q.U.A.S.E.

A Figura 5 apresenta pontuação ajustada (PA), a qual foi definida para ponderar cliques entre simulações de dificuldades diferentes. O objetivo é atribuir penalidade maior para cliques em simulações mais fáceis relativamente a mais difíceis. As seguintes variáveis foram ajustadas experimentalmente: v, p, P, K, PA. Para facilitar a elaboração de simulações, foi criada uma escala qualitativa (EQ) para a facilitar a elaboração de testes de *phishing* e a comparação entre testes.

	P	1/P	PP(%) ((1/P)/min(1/P))-K (%)	PP ((1/P)/min(1/P))-K
min	7	0,14286	250%	2,50000
	8	0,12500	216%	2,16071
	9	0,11111	190%	1,90476
	10	0,10000	171%	1,70714
	11	0,09091	155%	1,55195
	12	0,08333	143%	1,42857
	13	0,07692	133%	1,32967
	14	0,07143	125%	1,25000
	15	0,06667	119%	1,18571
	16	0,06250	113%	1,13393
	17	0,05882	109%	1,09244
	18	0,05556	106%	1,05952
	19	0,05263	103%	1,03383
	20	0,05000	101%	1,01429
max	21	0,04762	100%	1,00000

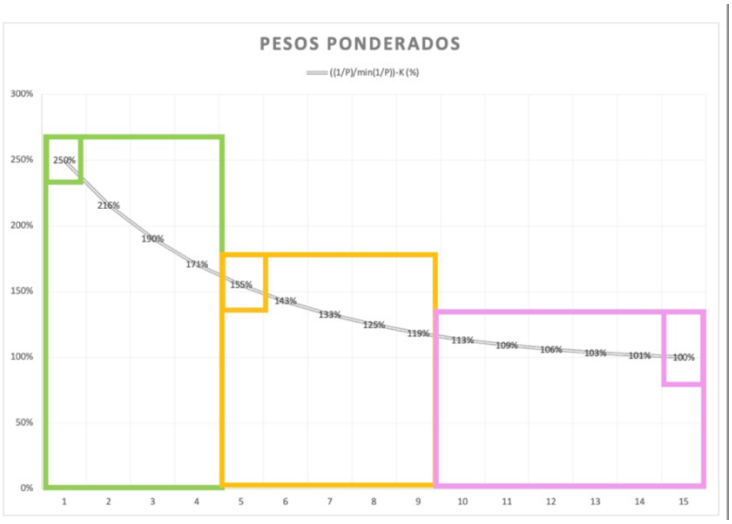

Figura 5 - Pontuação ajustada (PA) aplicada na metodologia Q.U.A.S.E.

5. Resultados e discussões

5.1. Testes de *phishing*

Os resultados são apresentados na Figura 6 dos treinamentos realizados em 2022 e 2023, respectivamente. Em todas as avaliações o resultado apontou para melhora em relação aos testes realizados antes (T1) e depois (T3) do treinamento, o que evidenciou cumprimento de objetivo para a metodologia proposta para aprimoramento da consciência em relação à detecção de ataques de *phishing* empregando a metodologia Q.U.A.S.E.

	F/R(%)	1/P	PA	s
teste (T = 1)	46,67	0,05	1,01429	47,33333
	8,889	0,07142857	1,25000	11,11111
	2,222	0,08333333	1,42857	3,17460
	2,222	0,125	2,16071	4,80159
teste (T = 3)	6,522	0,05	1,01429	6,61491
	2,174	0,07142857	1,25	2,7173913
	2,174	0,08333333	1,428571429	3,10559006
	2,174	0,125	2,160714286	4,69720497

T1	47,33333
T3	17,13509

	F/R(%)	1/P	PA	s
teste (T = 1)	60	0,05263158	1,03383	62,03008
	12,5	0,07142857	1,25000	15,62500
	0	0,09090909	1,55195	0,00000
	14,28571	0,11111111	1,90476	27,21088
teste (T = 3)	40	0,05263158	1,03383	41,35338
	0	0,07142857	1,25000	0,00000
	0	0,09090909	1,55195	0,00000
	0	0,11111111	1,90476	0,00000

T1	104,86596
T3	41,35338

Figura 6 – Resultados finais obtidos em diferentes avaliações

Em termos de resultados alcançados, observa-se que em todos os casos T3>T1 (vide Figura 6), o que significa situação melhora de prontidão dos usuários em relação aos testes realizados antes e depois do treinamento. Sob o ponto de vista de riscos de segurança cibernética, infere-se cenário de mitigação da probabilidade de materialização de riscos relacionados à postura dos usuários finais frente a mensagens de *phishing*.

Importante destacar que ao longo do tempo, o modelo passou por pequenos ajustes. Dentre os quais, destaca-se a simplificação de seis para cinco critérios e a adaptação do acrônimo para o português, facilitando a memorização. Ressalta-se que em 2024 os testes de *phishing* alçaram patrocínio para ser realizado para todo o TCU, em forma de campanha. Como esclarecido na metodologia, a pontuação final não foi considerada para fins de avaliação. Por outro lado, para que teve oportunidade de ter acesso à página de aterrissagem (*landing page*), após clicar em alguma simulação, foi convidado para a realizar treinamento previsto para turma a ser realizada em 2025.

Portanto, mesmo sendo um modelo simples e de fácil memorização, o Q.U.A.S.E. tem mostrado eficácia em oferecer resultados de melhoria da prontidão de usuários frente a testes de *phishing* em cenários reais.

5.2. Comparação com outros modelos - NIST

A cartilha *NIST Phish Scale* [Dawkins and Jacobs 2023] foi publicada mais de um ano depois, em novembro de 2023. De certa forma, mostrando que o modelo proposto estava em caminho adequado. Contudo, esta cartilha é organizada em dez critérios e organizados em difícil memorização. Há basicamente dois grupos de categorias. Pistas observáveis e alinhamento de premissas.

A categoria de pistas observáveis (*cues*) possui cinco grupos principais. a) Erros: indicadores de erros ortográficos e gramaticais e inconsistências. b) Indicadores técnicos:

tipo de anexo, nome do remetente, endereço de e-mail, links (URL) e uso falsificação de domínio (spoofing). c) Apresentação visual: foca em aspectos visuais, como ausência ou imitação de logotipos e marcas, designs ou formatações pouco profissionais, além de ícones e indicadores de segurança falsos. d) Linguagem e conteúdo: inclui abordagem ameaçadora, saudação genérica. e) Táticas comuns: inclui apelos humanitários, ofertas "boas demais para serem verdade", tentativas de fazer o destinatário se sentir especial, ofertas limitadas no tempo, imitações de processos de trabalho ou negócios.

A segunda categoria diz respeito ao alinhamento de premissas, sendo uma medida de quão próximo um e-mail corresponde às funções de trabalho ou responsabilidades do destinatário, com os seguintes critérios: a) Imita prática no local de trabalho, como procedimentos internos ou interações frequentes. b) Verificação se o conteúdo é relevante para as atividades diárias do destinatário, aumentando a probabilidade de que ele seja considerado legítimo. c) Avaliação em contexto mais amplo, incluindo situações que também ocorram fora do ambiente de trabalho. d) Análise se o e-mail induz o usuário a agir rapidamente, insinuando que haverá consequências negativas caso não tome a ação. e) Verificação se o usuário já realizou treinamento específico, capaz de influenciá-lo na identificação do e-mail. Por isso, o último elemento é subtraído e não somado, ao contrário dos demais.

A pontuação final é o resultado da soma das categorias. Em geral, quanto menos pistas o e-mail contiver e mais forte for o alinhamento das premissas com a organização, mais difícil seria detectá-lo como *phishing*, em tese. Inversamente, quanto mais pistas e mais fraco for o alinhamento das premissas de um e-mail, mais fácil será associá-lo como um *phishing*.

Portanto, em relação à cartilha publicada pela renomada organização normativa americana, a metodologia Q.U.A.S.E. possui metade dos critérios e baixa complexidade de memorização, adotando mnemônico de fácil memorização. Como dito anteriormente, a primeira versão do Q.U.A.S.E. foi criada no primeiro semestre de 2022, por ocasião da organização primeira turma temática.

5.3. Comparação com outros modelos - CISA

O documento intitulado *Update to Phishing General Security Postcard* foi publicado em janeiro de 2024, também posteriormente à primeira versão do modelo proposto. Trata-se de uma cartilha resumida sobre orientações para identificar ataques de *phishing*, bem como explicar como reportar incidentes e mitigar riscos [CISA-FBI 2024].

A metodologia é simples e apenas baseadas em 5 passos: a) Endereço de remetente suspeito, que pode imitar uma empresa legítima; b) Saudações e assinaturas genéricas, bem como falta de informações de contato no bloco de assinatura; c) Hiperlinks que não correspondem ao texto (quando se passa o mouse sobre eles); d) Erros ortográficos, gramaticais e formatação inconsistente; e) Anexos suspeitos ou solicitações para baixar e abrir um anexo.

Apesar de conter apenas cinco critérios de diagnóstico, o guia carece de elementos metodológicos. Não há um modelo de pontuação ou ranking. Apenas a recomendação para proceder testes de *phishing*, como uma das medidas protetivas. Ademais, o guia também recomenda outras medidas, como: autenticação multifator (MFA), gerenciadores de senhas, segmentação dos servidores de correio eletrônico de outros ativos críticos

5.4. Comparação com outros modelos – MS-ISAC

O documento anexado intitulado *Phishing Guidance: Stopping the Attack Cycle at Phase One* foi publicado em outubro de 2023, portanto também posterior à primeira versão do modelo proposto, pela MS-ISAC (*Multi-State Information Sharing and Analysis Center*). Fornece guia detalhado de orientações para fazer frente a ataques de *phishing* [MS-ISAC 2023].

O guia não oferece uma metodologia baseada em pontuação. Orienta de forma geral a adoção de medidas protetivas contra *phishing*, sob duas vertentes: obtenção de credenciais e infecção por *malware*.

Portanto, o documento não se enquadraria no escopo de análise e foi mencionado como parte integrante do esforço de coleta de dados. A Tabela 1 oferece uma comparação geral entre os modelos analisados.

Tabela 1 - Comparação entre modelos analisados.

Modelo	Critérios	Avaliação	Observação
Q.U.A.S.E.	5	Sim	Simples e fácil adesão por usuários finais
NIST	10	Sim	Complexo para usuários finais
CISA	5	não possui	Carece de elementos metodológicos
MS-ISAC	nenhum	não possui	Foco em medidas protetivas, não sendo útil para diagnóstico em usuários finais

6. Conclusão e trabalhos futuros

Como conclusão, a metodologia Q.U.A.S.E. demonstrou como a simplicidade pode gerar bons resultados. Ao condensar a detecção de *phishing* por usuários finais em apenas cinco critérios de fácil memorização, apresentou resultados frente a padrões de mercado posteriormente publicados como o *NIST Phish Scale*, com dez itens de avaliação.

O objetivo principal da proposta foi criar uma metodologia prática, de rápida aplicação e baixo custo de treinamento, capaz de fortalecer a consciência de usuários finais frente a ameaças de *phishing* no ambiente organizacional.

Além disso, entregou benefícios tangíveis, elevando indicadores de prontidão de usuários (T3>T1 – Figura 6) em treinamentos anuais realizados no TCU. Os resultados alcançados nos ciclos de 2022 e 2023 demonstraram que a abordagem foi eficaz em promover melhoria real no comportamento dos usuários.

Como trabalhos futuros, o treinamento acerca de *phishing* foi incluído no planejamento do Tribunal para 2025, como parte integrante de campanha temática de conscientização de usuários acerca de *phishing* com abrangência ampla para todo o órgão. Pretende-se também promover intercâmbio de informações com outros órgãos.

Além disso, planeja-se evoluir o modelo, incorporando sugestões e críticas principalmente dos participantes; aprofundar a análise do desempenho de diferentes perfis de usuários e explorar o desenvolvimento de módulos complementares; os quais serão

fundamentais para assegurar evolução e alinhamento às mudanças nas ameaças cibernéticas e nos comportamentos dos usuários, bem como buscar parceiras com outros órgãos públicos a fim de trazer sinergia de trabalhos de interesses afins e colaborar para o serviço público de forma ampla.

Por outro lado, é importante reconhecer algumas limitações do estudo: a aplicação restringe-se a um órgão público, o que limita a generalização ampla dos resultados até o momento. Espera-se aprimorar o cronograma de execução de simulações, tendo em vista que depende de negociação interna. Além disso, será proposto avaliar a contratação de plataforma que permita agregar abordagens orientadas à gamificação, bem como o aprimoramento das simulações para que possa fazer frente a novos tipos de ameaças.

7. Referências

AICD (2022). Cyber Security Governance Principles. Australian Institute of Company directors (AICd) and the Cyber Security Cooperative research Centre (CSCrC). https://www.aicd.com.au.

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet 2020*, v. 12, n. MDPI, p. 168.

Bassett, G., Hylender, D., Langlois, P., Pinto, A. and Widup, S. (2022). Verizon Data Breach Investigations Report (DBIR). Verizon. www.verizon.com.

Caridi, C., Dwyer, J., Emerson, R. and Singleton, C. (feb 2024). X-Force Threat Intelligence Index 2024. . IBM. https://www.ibm.com/reports/threat-intelligence.

CISA-FBI (2024). Update to Phishing General Security Postcard. CISA - Cybersecurity and Infrastructure Security Agency - FBI | MS-ISAC | ACSC | NCSC-UK | CCCS | ANSSI | BSI | CERT NZ | NCSC-NZ. https://www.cisa.gov.

Dawkins, S. and Jacobs, J. (nov 2023). NIST Technical Note 2276 - Phish Scale - user guide. NIST (National Institute of Standards and Technology). https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2276.pdf.

Ell, M. (2024). Cyber Security Breaches Survey - Official Statistics. . GOV.UK. https://www.gov.uk.

FBI (2023). Internet Crime Report. Internet Crime Compliant Center (IC3) - Federal Bureau of Investigation (FBI). https://www.ic3.gov.

Herzog, P. (2016). The Open Source Cybersecurity Playbook. Institute for Security and Open Methodologies (ISECOM)/Barkly. https://www.isecom.org.

Johns, E. (2023). Cyber Security Breaches Survey - Official Statistics. . GOV.UK. https://www.gov.uk.

Lella, I., Tsekmezoglou, E., Theocharidou, M., Magonara, E. and Malatras, A. (2024). ENISA Threat Landscape (ETL) Report. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu.

McCabe, E. (2023). Blueprint for Ransomware Defense. ISACA. https://www.isaca.org/resources/white-papers/2023/blueprint-for-ransomware-defense.

Merritt, M. et al. (2024). *NIST Special Publication 800-50r1*. National Institute of Standards and Technology.

Mimecast (2024). The State of Email & Collaboration Security Report 2024. Mimecast. https://assets.mimecast.com/api/public/content/state-of-email-and-collaboration-security-2024?v=a345394e.

MOURA, Gerges de; OERTING, Troels (2019). The Cybersecurity Guide for Leaders in Today's Digital World. World Economic Forum (WEF).

MS-ISAC (2023). Phishing Guidance - Stopping the Attack Cycle at Phase One. . The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC). https://www.cisa.gov.

Radicati (2024). Email Statistics Report, 2021-2025. The Radicati Group, Inc. https://www.radicati.com.

Siadati, H. et al. (2017). Measuring the Effectiveness of Embedded Phishing Exercises.https://www.researchgate.net/publication/319128761_Measuring_the_Effectiveness_of_Embedded_Phishing_Exercises.

Sjouwerman, S. (2024). Which phishing emails fooled the most people. *KnowBe4*. https://blog.knowbe4.com.

Terranova (2024). Phishing Benchmark Global Report. Microsoft; Terranova Security. https://www.terranovasecurity.com/gone-phishing-tournament.