ISURESEARCH (2025), Vol. 3, N°1, págs. 22 – 26
https://www.isutc.ac.mz/?p=12499

Estudo sobre hacking ético na prevenção de ciberataques: uma simulação de Phishing baseada em Nuvem para conscientização em Cibersegurança

Leandro Tito Manjate*

Departamento de Tecnologias da Informação e Comunicação, Instituto Superior de Transportes e Comunicações, Prol. Av. Kim Il Sung, Maputo, Moçambique

*e-mail do autor correspondente: titomanjate@gmail.com

***Resumo* – O phishing representa um método prevalente de ataques cibernéticos, que se aproveita de vulnerabilidades humanas em vez de deficiências técnicas. Este estudo ilustra como métodos de hacking ético, combinados com simulações realistas baseadas em nuvem, podem aprimorar a conscientização sobre segurança cibernética e diminuir a vulnerabilidade ao cibercrime. A configuração foi estabelecida na Amazon Web Services (AWS), com o Route 53 para administração de DNS, uma instância EC2 e o GoPhish conectado ao Mailgun para entrega de e-mails. Duas ferramentas de hacking ético baseadas em Python — um keylogger e um backdoor reverso — foram criadas para demonstrações regulamentadas. Dois questionários avaliaram os níveis de alfabetização digital e as opiniões dos utilizadores sobre segurança cibernética e hacking ético. Os resultados indicaram uma falta de compreensão das ameaças de engenharia social e consideráveis suscetibilidades comportamentais em exercícios simulados de phishing. A pesquisa sugere que o hacking ético, implementado em um arcabouço formal como a ISO/IEC 27001, é um instrumento eficaz para cultivar uma cultura robusta de segurança cibernética.**

Palavras-chave *- Hacking Ético; Phishing; Conscientização em Ciberseguran-ça; Segurança em Nuvem; ISO 27001.*

I. INTRODUÇÃO

O cibercrime aumentou dramaticamente na última década, com o *phishing* representando uma parcela significativa de roubo de identidade e perdas financeiras globalmente (Ferreira & Teles, 2019; Asfoor et al., 2020). Os perpetradores estão cada vez mais utilizando comunicação persuasiva, sites falsificados e táticas de engenharia social para enganar os consumidores e fazê-los revelar informações confidenciais. Em diversas economias emergentes, como Moçambique, a conscientização e as medidas tecnológicas são inadequadas para lidar com essas dificuldades.

O *hacking* ético oferece uma estrutura legal e instrutiva para identificar vulnerabilidades antes que sejam exploradas por agentes maliciosos (Hadnagy, 2022). A realização de simulações controladas que replicam ataques reais permite a observação das respostas dos utilizadores, a avaliação de vulnerabilidades e a identificação de áreas de falha, tanto nos aspetos humanos quanto tecnológicos.

Este projeto visa avaliar como as técnicas de *hacking* ético, nomeadamente simulações de *phishing*, podem melhorar a conscientização sobre segurança cibernética. Os objetivos primários são:

- Desenvolver uma plataforma de *phishing* baseada em nuvem que integra configurações técnicas autênticas com análise comportamental;
- Avaliar a vulnerabilidade do utilizador através de interações observadas e pesquisas;
- Fornecer uma abordagem adequada para ambientes académicos e corporativos em Moçambique.

O documento está organizado da seguinte forma: A Secção II delineia a técnica; a Secção III articula os resultados experimentais; a Secção IV analisa as descobertas; a Secção V encerra com recomendações.

1.1. Revisão da Literatura

A literatura científica demonstra, de forma consistente, que os ataques de *phishing* continuam a ser o vector de ataque mais prevalente contra utilizadores em ambientes corporativos e académicos. Estudos como os de Asfoor et al. (2020) e Ferreira & Teles (2019) evidenciam que factores comportamentais — incluindo excesso de confiança, baixa literacia digital e heurísticas simples de decisão — contribuem mais para o sucesso do *phishing* do que falhas tecnológicas.

As simulações de *phishing* são amplamente utilizadas para medir vulnerabilidades humanas, sendo plataformas como o *GoPhish* empregues em universidades e organizações para avaliar respostas comportamentais (Redmiles et al., 2020). A investigação demonstra que estudantes da área de Tecnologias de Informação apresentam, frequentemente, maior propensão ao erro devido a um fenómeno conhecido como *overconfidence bias*, documentado por Rajivan et al. (2018), que descreve a tendência de utilizadores tecnicamente competentes ignorarem indicadores de risco por acreditarem reconhecer ameaças com maior facilidade.

Adicionalmente, estudos recentes (Hadnagy, 2022; Heartfield & Loukas, 2016) demonstram que a utilização de metodologias de *hacking* ético em ambiente controlado melhora significativamente a retenção de conhecimento,

uma vez que coloca o utilizador numa situação realista e emocionalmente envolvente, reforçando a aprendizagem experiencial.

A investigação relativa ao protocolo *HTTPS* também revela um equívoco amplamente disseminado: Felt et al. (2016) mostram que mais de metade dos utilizadores acredita que o cadeado de "site seguro" garante legitimidade, o que facilita ataques de *phishing* com domínios fraudulentos, mas certificados TLS válidos. Assim, a confusão observada nesta pesquisa (54,5%) é consistente com achados internacionais.

II. METODOLOGIA

Na presente secção, são descritos de forma detalhada os procedimentos metodológicos adotados no estudo, incluindo a configuração da infraestrutura, as ferramentas de *hacking* ético utilizadas, o desenho da campanha de *phishing*, os questionários aplicados e as considerações éticas e legais que orientaram a condução da investigação.

A. Configuração da Infraestrutura

O ambiente de simulação de *phishing* foi implementado na *Amazon Web Services* (AWS) utilizando uma instância *EC2 Ubuntu Server*. O *Apache2* forneceu o serviço web para as páginas de login clonadas, e o *Route* 53 cuidou do gerenciamento de *DNS*. Um nome de domínio dedicado foi registado e protegido com certificados *SSL/TLS* via *Certbot* para garantir a comunicação criptografada e aumentar o realismo (Manjate, 2024; OWASP, 2023).

A *Mailgun* cuidou da entrega de e-mails e da análise de dados (rastreamento de aberturas/cliques). A arquitetura do ambiente simulado está está ilustrado na Figura 1.

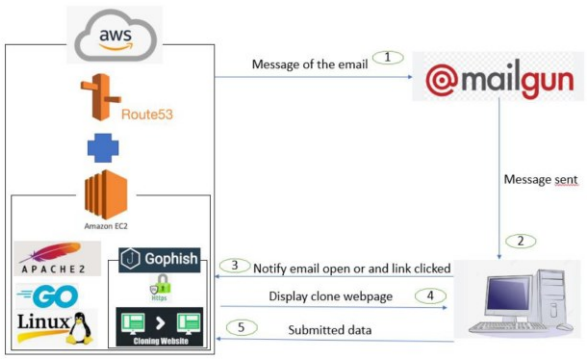

Figura 1. Arquitetura do ambiente de simulação de phishing baseado em nuvem, integrando AWS (EC2, Route 53), Apache2, GoPhish e Mailgun para entrega e rastreamento de e-mails.

B. Ferramentas de *Hacking* Ético

Duas ferramentas *Python* foram criadas exclusivamente para fins didáticos:

- *Keylogger* – registou as teclas digitadas para ilustrar vulnerabilidades de vazamento de dados em endpoints não seguros;
- *Reverse Backdoor* – simulação de execução de comandos após comprometimento, enfatizando as fases de pós-exploração.

Ambos foram executados exclusivamente em máquinas virtuais isoladas, desprovidas de qualquer conexão com sistemas de produção.

Importa salientar que o *keylogger* e o *reverse backdoor* produzidos foram utilizados exclusivamente para demonstração em ambiente isolado. Nenhuma destas ferramentas foi executada nos dispositivos dos participantes, e não houve qualquer tentativa de recolher credenciais reais. O seu propósito foi exclusivamente didático, para ilustrar fases de pós-exploração no contexto de formação em cibersegurança.

C. *Design* de Campanha de *Phishing*

O *GoPhish* (Figura 2) ofereceu uma estrutura para o desenvolvimento de campanhas de *phishing* autênticas (GoPhish, 2024). Os perfis dos remetentes foram concebidos para imitar endereços institucionais, enquanto os modelos de mensagens emulavam comunicados internos. Cada *e-mail* continha um pixel de rastreamento e um *link* exclusivo para a página da *web* replicada. O sistema documentou se cada destinatário acessou, clicou ou forneceu informações.

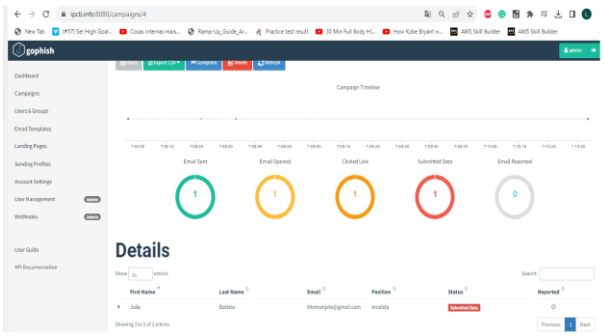

Figura 2. Painel de controle da campanha *GoPhish* exibindo o *status* de entrega de *e-mails*, rastreamento de aberturas/cliques e estatísticas de envio de credenciais para cada simulação.

D. Questionários

Duas pesquisas online foram administradas:

- O Questionário. A: avaliou a compreensão de estratégias de engenharia social, protocolos de senhas e higiene da rede;
- O Questionário B: avaliou as perceções sobre *hacking* ético, cibercrime e responsabilidade legal.

Um total de 44 participantes concluíram ambos os questionários. As respostas foram recolhidas através do *Google Forms* e exportadas em formato *CSV* para posterior análise. De forma complementar, os resultados da simulação de *phishing* gerados pelo *GoPhish* — incluindo métricas de entrega, abertura, cliques e submissão de credenciais — foram igualmente exportados em formato *CSV*. A análise estatística foi realizada no *Microsoft Excel* e em *Python* (*pandas*), abrangendo o cálculo de frequências absolutas, percentagens, organização das respostas em escalas *Likert* e tabulação cruzada entre variáveis. Os resultados finais são apresentados sob a forma de valores percentuais e tabelas.

E. Considerações Éticas e Legais

Todas as simulações foram conduzidas sob aprovação ética. Os participantes foram informados sobre o propósito educacional do projeto e deram seu consentimento. Nenhum dado pessoal real ou credenciais foram mal utilizados, e todas as informações capturadas foram armazenadas de forma segura e anonimizadas.

III. RESULTADOS

A. Implementação Técnica

A infraestrutura validou com sucesso todas as configurações de *DNS* e *TLS*. A *Mailgun* confirmou a verificação do domínio, e os e-mails foram entregues com sucesso, com rastreamento de abertura e cliques activado. Isso garantiu alto realismo e rejeição mínima de spam.

B. Questionário A — Alfabetização Digital (n = 44)

A presente subsecção apresenta os resultados referentes à caracterização demográfica dos participantes (Tabela 1), ao seu nível de conhecimento em engenharia social (Tabela 2) e às suas práticas de segurança, incluindo os principais equívocos identificados (Tabela 3).

i) Demografia

A maior parte dos participantes são estudantes (84,10%) da área de ciências da computação (88,60%). O Género masculino (84,10%) foi dominante entre os participantes (Tabela 1),

Tabela 1 Caracterização Demográfica da Amostra (n = 44)

Variável	Categoria	Percentagem
Género	Masculino	84,10%
	Feminino	15,90%
Área de estudo	Ciencia de computação/TI	88,60%
	Outras áreas	11,40%
Situação académica	Estudantes	84,10%
	Profissionais	15,90%

ii) Conscientização sobre engenharia social

Tabela 2. Conscientização dos Participantes sobre Conceitos de Engenharia Social (n = 44)

Indicador Avaliado	Percentagem
Identificaram o termo “engenharia social”	77,30%
Reconheceram ataques “shoulder surfing” e “quid pro quo”	90,90%
Identificaram correctamente o acto de “tailgating”	70,50%
Reconheceram o “vishing” (phishing por voz)	43,20%
Conheciam o “pretexting”	81,60%
Identificaram o phishing	75,00%

Os dados sobre conscientização sobre os conceitos de engenharia social (Tabela 2) usados como indicador indicam que a maior parte do participantes (acima de 50%) estão familiarizados com os termos (indicadores avaliados). Contudo, os resultados sugerem, também, que somente cerca de 43% reconhecem o termo “*vishing*” (*phising* por voz).

iii) Práticas de segurança e equívocos

Tabela 3. Práticas de Segurança e Equívocos dos Participantes (n = 44)

Indicador Avaliado	Percentagem
Recusariam chamadas suspeitas solicitando dados pessoais	50,00%
Compreenderam o papel das perguntas de segurança	79,50%
Acreditavam incorretamente que páginas HTTPS são sempre seguras	54,50%
Reconheceram o risco de partilhar dados em redes sociais	90,90%
Consideraram inseguro partilhar palavras-passe	97,70%
Apoiaram o uso de autenticação de dois factores (2FA)	90,90%

Em relação às práticas de segurança (Tabela 3), acima de 90% dos participantes reconhecem como sendo práticas inseguras a partilha de dados em redes sociais (90,90%) e a partilha de palavra passe (97,70%), enquanto 90,90% apoiariam uso da autenticação por dois factores.

C. Questionário B — Percepções sobre Hacking Ético

Este questionário foi desenvolvido para avaliar as percepções, a conscientização e a compreensão dos participantes sobre o *hacking* ético como uma abordagem legítima e preventiva para combater o cibercrime. O objetivo foi explorar como os indivíduos diferenciam entre *hacking* ético e malicioso, seu nível de confiança em hackers éticos e sua opinião sobre a integração de práticas de hacking ético na educação em segurança cibernética.

A pesquisa consistiu em uma série de afirmações medidas através de uma escala *Likert* de cinco pontos, variando de Discordo Totalmente a Concordo Totalmente. As questões abordaram aspectos éticos do teste de penetração, limites legais do *hacking* ético e a importância percebida dos hackers éticos na proteção das organizações contra ameaças cibernéticas.

Tabela 4. Percepções dos Participantes sobre Hacking Ético (Escala Likert, n = 44)

Afirmação	Discordo Totalmente	Discordo	Neutro / Incerteza	Concordo	Concordo Totalmente
O hacking ético ajuda a identificar vulnerabilidades antes que cibercriminosos as explorem	0%	2%	14%	48%	36%
Existem incertezas sobre os limites legais e éticos do hacking ético	4%	4%	16%	50%	26%
Programas de hacking ético devem ser integrados na educação formal	3%	3%	22%	41%	31%
Existe risco de uso indevido das competências de hacking ético sem supervisão	2%	4%	6%	58%	30%

Os resultados (Tabela 4) demonstraram que 84% dos participantes concordaram ou concordaram fortemente que o *hacking* ética ajuda a identificar vulnerabilidades antes que cibercriminosos as explorem. Isso demonstra um alto nível de aceitação e compreensão do *hacking* ético como uma medida de segurança proativa. Contudo, 16% dos respondentes expressaram incerteza em relação às limitações legais e éticas dos testes de penetração, indicando uma falta parcial de conhecimento sobre as regulamentações nacionais ou institucionais.

Curiosamente, mais de 70% dos entrevistados apoiaram a integração de programas de *hacking* ético e conscientização sobre segurança cibernética na educação formal, acreditando que isso ajudaria a fortalecer uma cultura digital responsável e orientada para a segurança. Uma parcela menor (cerca de 6%) levantou preocupações sobre o potencial uso indevido das habilidades de *hacking* ético, caso não sejam devidamente supervisionadas ou regulamentadas.

No geral, esses resultados destacam uma percepção geralmente positiva sobre o *hacking* ético entre os participantes, reconhecendo-o como um componente essencial das estratégias modernas de segurança cibernética.

No entanto, os resultados também enfatizam a necessidade de campanhas de conscientização contínuas, legislação mais clara e estruturas éticas padronizadas para garantir que as práticas de *hacking* ético sejam conduzidas de forma responsável e transparente.

D. Resultados da Campanha de *Phishing*

A presente subsecção apresenta os resultados da simulação de *phishing* obtidos nas coortes de Tecnologias de Informação (TI; Tabela 5) e Não-TI (Tabela 6).

Tabela 5. Resultados da Campanha de Phishing na Coorte de TI (n = 17)

Métrica	Valor
E-mails enviados	17
E-mails abertos e clicados	5 (29,4%)
Envios de credenciais	2 (11,8%)

Tabela 4. Resultados da Campanha de Phishing na Coorte Não-TI (n = 17)

Métrica	Valor
E-mails enviados	17
E-mails abertos e clicados	5 (29,4%)
Envios de credenciais	1 (5,9%)

Os resultados demonstram níveis de curiosidade semelhantes entre ambos os grupos (Tabelas 5 e 6), mas uma taxa de submissão mais elevada entre os estudantes de TI (Tabela 6) — possivelmente devido a uma excessiva confiança em sua capacidade de identificar conteúdo falso.

IV. DISCUSSÃO

Os resultados confirmam que os factores humanos permanecem o elemento mais fraco em cibersegurança. Mesmo entre estudantes de TI, que possuem conhecimento técnico, vulnerabilidades comportamentais persistiam. Taxas de cliques iguais entre as coortes (29,4%) demonstram que treinamento e conscientização técnica, por si sós, não são suficientes sem testes contínuos.

A concepção equivocada de que *HTTPS* garante legitimidade (54,5%) é alarmante e reflete uma ampla incompreensão dos indicadores de confiança. Destaca-se a necessidade de programas de conscientização direcionados, que expliquem a falsificação de certificados e a personificação de domínios.

A prática de *hacking* ético demonstrou ser uma ferramenta pedagógica poderosa, oferecendo experiência prática e feedback realista. Simulações controladas como estas permitem que os utilizadores aprendam por meio da participação, em vez de apenas pela teoria, reforçando a retenção e a mudança de comportamento.

As limitações desta pesquisa incluem a pequena amostra focada em estudantes e as restrições éticas das campanhas simuladas, o que pode reduzir o realismo em comparação com ataques reais. Estudos futuros devem se estender aos setores corporativos e incluir painéis de conscientização automatizados para o acompanhamento do desempenho.

V. CONCLUSÃO

Este estudo demonstrou com sucesso que o *hacking* ético, implementado através de simulações controladas de *phishing* baseadas em nuvem, pode identificar vulnerabilidades humanas e aprimorar a conscientização sobre segurança cibernética.

Principais resultados:

- Tanto os participantes de *TI* quanto os não participantes de *TI* exibiram níveis de curiosidade semelhantes, refletidos em taxas de cliques iguais (29,4%);
- Concepções errôneas sobre *HTTPS* e excesso de confiança entre utilizadores técnicos aumentaram a exposição;
- O *hacking* ético, quando utilizado de forma ética e legal, é uma metodologia eficaz de conscientização alinhada aos princípios da ISO/IEC 27001.

Os achados deste estudo alinham-se com pesquisas internacionais que demonstram que o erro humano é o principal vetor de ataques bem-sucedidos. Trabalhos de Redmiles et al. (2020) documentam taxas de clique semelhantes entre utilizadores com formação técnica e não técnica, sugerindo que conhecimentos prévios não eliminam vulnerabilidades comportamentais. O elevado nível de confiança dos estudantes de TI encontrado neste estudo também foi identificado por Rajivan et al. (2018), que descrevem excesso de confiança como um preditor significativo de falhas em avaliações de *phishing*.

Da mesma forma, a confusão observada em relação ao *HTTPS* é amplamente relatada em literatura. Felt et al. (2016) demonstram que os utilizadores frequentemente interpretam o cadeado SSL como prova inequívoca de autenticidade, ignorando que certificados TLS podem ser obtidos para domínios maliciosos. Assim, os resultados deste estudo reforçam um problema global, não local.

Recomendações:

1. Realizar simulações trimestrais de *phishing* com micro-treinamentos direcionados aos utilizadores que clicarem em links;
2. Implementar autenticação de dois factores e políticas de senhas mais robustas;
3. Adoptar SPF, DKIM e DMARC para autenticar e-mails e evitar falsificação;
4. Integrar módulos de hacking ético nos currículos do ensino superior;
5. Estabelecer marcos legais claros para testes de penetração autorizados.

AGRADECIMENTOS

O autor expressa sincera gratidão ao Instituto Superior de Transportes e Comunicações (ISUTC) pelo apoio académico e a todos os participantes que contribuíram para este estudo. Agradecimentos especiais aos supervisores e mentores por sua orientação e incentivo ao longo deste projecto.

REFERÊNCIAS

Asfoor, A. H., Abdul Rahim, F., & Yussof, S. (2020). Identifying factors that influence security behaviours relating to phishing attack susceptibility: A systematic literature review. Journal of Theoretical and Applied Information Technology, 98(15), 3127–3161.

Ferreira, A., & Teles, F. (2019). Human factors in phishing attacks: A systematic literature review. Computers in Human Behavior, 92, 162–175.

GoPhish. (2024). Open-Source Phishing Framework. https://getgophish.com.

Hadnagy, C. (2022). Social Engineering: The Science of Human Hacking (2.ª ed.). Wiley.

ISO. (2022). ISO/IEC 27001: Information Security Management Systems — Requirements. International Organization for Standardization.

Manjate, L. T. (2024). Ethical Hacking Study Against Cybercrime [Master's dissertation, Instituto Politécnico de Castelo Branco].

OWASP Foundation. (2023). OWASP Testing Guide v5. https://owasp.org

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2020). Where is the digital divide? Measuring phishing susceptibility across socioeconomic groups. Proceedings of the 29th USENIX Security Symposium.

Rajivan, P., Gonzalez, C., & Loya, P. (2018). Decision-making and overconfidence in phishing attack detection. Frontiers in Psychology, 9, 1593.