CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Práticas de educação não-formal:

Phishing

R2 CYBER TOOLKIT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

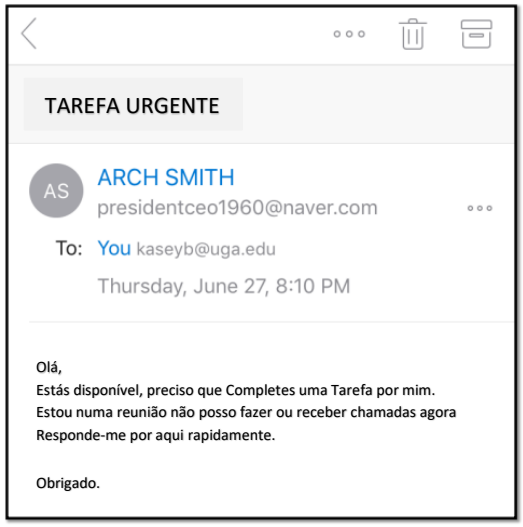
#9	**Há Algo Suspeito**
Ameaça(s)	Phishing
	Os ataques de phishing envolvem frequentemente e-mails, mensagens ou websites fraudulentos, concebidos para se fazerem passar por organizações legítimas, como bancos, plataformas de redes sociais ou agências governamentais. Estas comunicações enganosas levam normalmente os destinatários a divulgar informações confidenciais, como credenciais de início de sessão ou números de contas financeiras, sob falsos pretextos. Os cibercriminosos recorrem a esta informação roubada para cometer roubo de identidade, fraude financeira ou outras atividades maliciosas, criando riscos significativos para a privacidade dos indivíduos (Roubo de Identidade e Fraude), finanças e segurança online.
Tipologia	*Exercícios de simulação*
Duração	Em minutos 2x40
Modalidade	Presencialmente [contexto de sala de aula]
Finalidade	Esta aula demonstra como os burlões tentam obter informação pessoal através de phishing. Frequentemente, a comunicação eletrónica, como e-mails e mensagens de texto, pode parecer proveniente de uma fonte fidedigna quando na realidade é fraudulenta.
Objetivos de aprendi-zagem	Após participar nesta aula, os estudantes serão capazes de: • Identificar as caraterísticas da comunicação eletrónica fidedigna • Explicar a importância de entender como evitar tentativas de phishing • Distinguir entre mensagens legítimas e fraudulentas e tentativas de phishing
Perfil do formando	13-17 anos
n° de participantes	Preferencialmente até 20 participantes, ou alunos de, no máximo, uma turma
Materiais	São necessários os seguintes materiais e recursos para esta aula: • Exemplos de phishing (ver anexo, ou imprimir os seguintes exemplos aqui - fonte: https://blog.usecure.io/the-most-common-examples-of-a-phishing-email#Email-account-upgrade-scam)
Preparação	Em preparação para esta aula, os formadores devem: • Rever o plano de aula • Imprimir os exemplos de phishing
Implementação	**Terminologia:** Os seguintes termos serão discutidos no decorrer da aula: • **Password**: a combinação de letras, números, e caracteres do teclado que devem ser introduzidos com vista a aceder a diversos serviços online (e-mail, contas de redes sociais, contas para compras online, etc.) • **Phishing**: a tentativa fraudulenta de obter informação confidencial como nomes de utilizador, palavras-passe, e dados de cartão de crédito, fazendo-se passar por uma entidade fidedigna numa comunicação eletrónica. **Informação Geral**:

	Implementação: (10 minutos) Phishing é a tentativa fraudulenta de obter informação confidencial, como nomes de utilizador, palavras-passe, e dados de cartão de crédito, fazendo-se passar por uma entidade fidedigna numa comunicação eletrónica. Por vezes, estes e-mails ou mensagens de texto aparentam provir de uma fonte legítima e possuem geralmente um caráter de urgência. As ligações presentes em e-mails de phishing encaminham, frequentemente, o utilizador para um website não fiável, com o objetivo de inserir informação confidencial. Os riscos associados com as tentativas de phishing incluem a obtenção de palavras-passe, a imitação do indivíduo para aceder a uma conta bancária e outros serviços financeiros, a compra de artigos online, a imitação do individuo em páginas de redes sociais, e o acesso a informação privada no computador do próprio. **Atividade 1: O que é Phishing?** Distribuir exemplos de phishing. Trabalho em grupos (20 minutos) - divida os estudantes em pequenos grupos de 4 alunos e forneça exemplos de phishing (ver anexo). Os estudantes possuem a tarefa de descrever cada um dos exemplos, quer se trate de fraude ou não. Se sim, porquê? Apresentação dos resultados dos alunos - (20 minutos) Clarificar e explicar - (10 minutos) **Atividade 2: Gerir Tentativas de Phishing** Porque se torna importante evitar tentativas de phishing? Por exemplo, um funcionário municipal inseriu os dados bancários da cidade e o cibercriminoso conseguiu transferir quase 800 000 euros da conta antes de alguém se aperceber do erro. Embora a cidade tenha um seguro e a fraude tenha sido denunciada às autoridades, é pouco provável que todo o dinheiro possa ser recuperado. Embora este exemplo se aplique a uma cidade, qualquer um pode ser vítima de uma tentativa de phishing. Utilize o *flip chart* e os marcadores para fazer brainstorming coletivo sobre as medidas a tomar se for vítima de uma tentativa de phishing. (10 minutos) Os exemplos incluem: • Não clicar em quaisquer ligações ou descarregar anexos. Estes podem conter vírus ou *spyware*. • Não responder ao e-mail ou mensagem de texto. • Marcar/categorizar o e-mail como “lixo” ou “spam”. • Se o e-mail fizer referência a uma conta e estiver preocupado com essa conta, contacte a empresa. No entanto, não utilize nenhuma das informações

	de contacto contidas no e-mail ou texto. Muitas vezes, estes criminosos criam números de telefone falsos. Verifique previamente as informações de contacto da empresa noutro local. • Reportar o e-mail de phishing às autoridades. **Atividade 3: Detetar as Tentativas de Phishing** Questionário para avaliar os conhecimentos - (10 minutos) pode ser realizado por todos, cada aluno pode fazê-lo de forma individual e, de seguida, partilhar os resultados com a turma. Embora a intenção seja para que a atividade desenvolva competências de privacidade e segurança relacionadas com a tecnologia, é importante que o formador conduza uma discussão de reflexão no final da aula. As possíveis perguntas de reflexão podem incluir: • Quais são algumas das caraterísticas das comunicações eletrónicas fidedignas? • Quais são algumas das caraterísticas das comunicações eletrónicas fraudulentas? • Porque se torna importante saber como evitar tentativas de phishing? • O que deves fazer após receberes um e-mail ou texto que pensas ser fraudulento?
Dicas e sugestões	Recomendamos a realização de testes de phishing com os alunos no final da aula. A hiperligação é o seguinte: https://phishingquiz.withgoogle.com/. https://phishingquiz.withgoogle.com/?hl=en https://www.proprofs.com/quiz-school/topic/phishing É uma ótima reflexão sobre os conhecimentos adquiridos.
Medidas de segurança	-
Referências externas e Recursos	• https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams •https://www.commonsense.org/education/digital-citizenship/lesson/dont-feed-the-phish • https://georgia4h.org/wp-content/uploads/Something-is-Phishy.pdf
Parceiro/ Autor	CPM- Centrum Prevencie Mladeze Slovakia

Anexo.

Distribuir exemplos de um e-mail de phishing e uma mensagem de texto de phishing.



Explicar o seguinte para o e-mail:

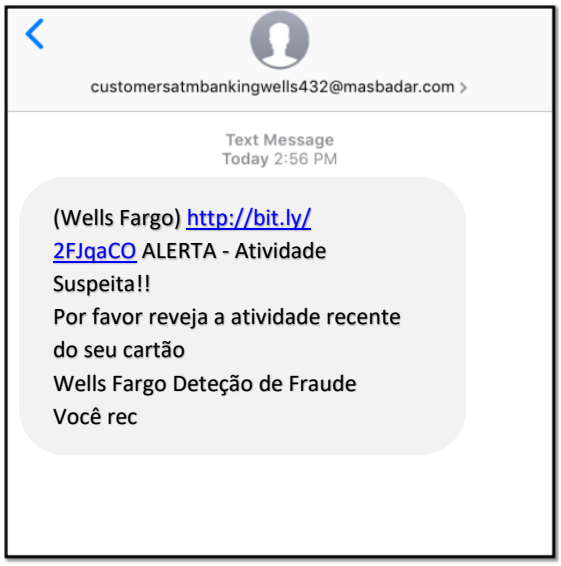
A funcionária (que trabalha para a Universidade da Geórgia) recebeu esta mensagem de e-mail. O seu supervisor é o Arch Smith, pelo que ela recebe e-mails dele com regularidade. Não obstante, após uma pesquisa mais profunda, existem caraterísticas suspeitas nesta mensagem:

• Apesar do e-mail ser de "Arch Smith", o endereço de e-mail utilizado não indica que foi o Arch a enviar a mensagem. Dado que a correspondência se encontra relacionada com o trabalho, torna-se também suspeito que não seja proveniente de uma conta de e-mail associada à Universidade da Geórgia.

• A ortografia, gramática e estrutura da mensagem de e-mail suscitam dúvidas. Palavras que se encontram-se em maiúsculas não deveriam estar. Em determinados casos, tanto a pontuação como a gramática estão incorretas.

• O e-mail não está assinado pelo Arch Smith. A generalidade dos e-mails termina com uma espécie de conclusão e assinatura.

• O e-mail parece deveras urgente e não refere em particular o motivo da urgência. O remetente também não se encontra disponível para atender chamadas telefónicas (o que seria considerado uma prática "comum" numa situação de emergência).



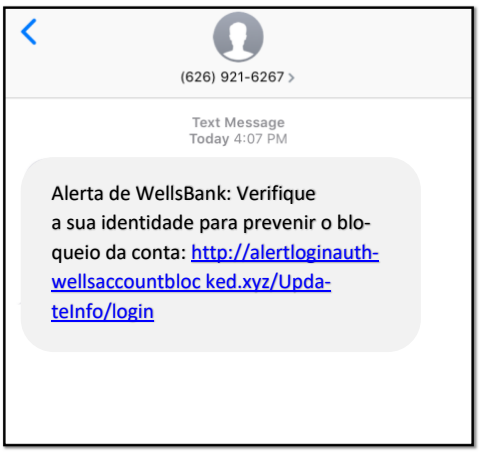
Explicar o seguinte para a mensagem de texto:

A pessoa possui uma conta bancária no Wells Fargo e, ocasionalmente, recebe atualizações do banco por e-mail. Não obstante, após uma pesquisa mais profunda, existem caraterísticas suspeitas nesta mensagem:

• O remetente desta mensagem utiliza o endereço de e-mail customersatmbankingwells432@masbadar.com. Não aparenta ser um endereço de e-mail legítimo associado à Wells Fargo.

• A hiperligação incorporada na mensagem constitui um url do bigly. O Bigly é um serviço que encurta urls - não exibindo o url completo do website. Embora muitos grupos utilizem estes serviços, só deve clicar no url encurtado quando conhece o remetente.

• A ortografia, gramática e estrutura do texto suscitam dúvidas. A mensagem não se encontra completa.



Um caso comum de obtenção de dados bancários online – Phishing, a tentativa fraudulenta de obter informação confidencial, como nomes de utilizador, palavras-passe, e dados de cartão de crédito, fazendo-se passar por uma entidade fidedigna numa comunicação eletrónica. Frequentemente, os indivíduos que respondem a este género de e-mails são convidados a realizar algo online que não os salvaguarda. Podem também ser convidados a clicar numa hiperligação e a partilhar informações. Por exemplo, pode ser-lhes pedido que partilhem a sua palavra-passe, informações financeiras, códigos PIN

ou que enviem dinheiro ou comprem artigos (como cartões de oferta). Muitas vezes, o momento é de urgência porque “foi detetada atividade suspeita” ou “a sua conta está bloqueada” até novas ações.

Algumas caraterísticas de um e-mail de phishing incluem:

• Necessidade de verificar as informações da conta (ex. conta de e-mail, conta bancária, conta de transferência de dinheiro, etc.). Muitas vezes, o e-mail diz que as suas informações pessoais expiraram ou necessitam de ser verificadas.
• Hiperligações na mensagem de e-mail/texto ou anexo. Normalmente, a hiperligação não fornece o URL, pelo que é difícil determinar para que website será redirecionado. De qualquer modo, clique apenas em hiperligações de remetentes com boa reputação.
• Sentido de urgência. Muitas vezes, os e-mails de phishing dão-lhe um período de tempo limitado (ex. 24 horas) para resolver um “problema” que não existe.
• Demasiado bom para ser verdade. As mensagens de e-mail de phishing podem prometer algum tipo de “retorno”, como dinheiro ou cartões de oferta, se realizar algo primeiro (normalmente, fornecer informações pessoais/confidenciais).
• Erros de ortografia, gramática e/ou estrutura. Uma gralha ocasional acontece numa mensagem de e-mail legítima, mas uma quantidade excessiva de erros indica uma mensagem de e-mail de phishing.
• Comprimento. Alguns e-mails de phishing tendem a ser curtos. Outros podem ser muito longos, explicando uma circunstância (ex. porque é que alguém não consegue fazer algo e porque é que precisa da sua ajuda).
• Saudação genérica. Muitos e-mails de phishing não têm uma saudação ou começam simplesmente com “olá”.

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.