European Crime Prevention Network (Rede europeia de prevenção do crime)

EUCPN Toolbox Series

N°. 13

Prevenção da fraude individual

Sumário executivo

A 13a toolbox da série publicada pelo Secretariado da EUCPN concentra-se na prevenção da *fraude individual.* A presidência da Bulgária (primeira metade de 2018) decidiu concentrar-se em:

"[…] *problemas relacionados com fraude, em particular golpes por telefone. Este tipo de crime tornou-se uma atividade criminosa lucrativa nos anos recentes, e tem vindo a desenvolver-se aos níveis nacional e transfronteiriço. Os grupos criminosos que se especializam nesta atividade estão a desenvolver-se de forma dinâmica e estão a afetar uma grande variedade de vítimas. Dada a participação ativa das vítimas e o seu envolvimento nos cenários criminosos e no efeito traumatizante sobre as mentes das vítimas, é necessário efetuar sérios esforços de prevenção, tendo em conta as especificidades a nível local, nacional e transfronteiriço".*

A fraude individual é um tipo de fraude em que os cidadãos regulares, individuais, estão a ser visados pelos criminosos. As vítimas são persuadidas a adotar uma mentalidade corporativa e, em seguida, são enganadas. Os nossos conhecimentos atuais sobre este tipo de fraude estão relacionados sobretudo com as suas formas contemporâneas, com o "phishing" como exemplo mais provável. No entanto, é importante reconhecer que a fraude individual já existe há muito mais tempo. As evoluções tecnológicas das últimas décadas simplesmente permitiram fazer com que estas fraudes sejam industrializadas a uma larga escala do que alguma vez se considerou possível. Quem nunca recebeu um e-mail de phishing na sua vida?

Conforme esclarecido na *justificativa* da presidência da Bulgária, as vítimas participam ativamente na sua vitimização. O ofensor tem por objetivo obter o dinheiro da vítima, mas ele só pode obter acesso ao dinheiro persuadindo a vítima. A tática essencial para convencer a vítima a participar nesta relação cúmplice é chamada **engenharia social**. Isto permite ao ofensor obter a confiança da vítima que é crucial para o sucesso da fraude. A psicologia social oferece-nos um melhor entendimento deste fenómeno. Apelando aos princípios sociais quotidianos e explorando essa "fraqueza humana", os infratores são capazes de ativar o que é chamado de segunda via de persuasão. A primeira via requer uma grande quantidade de pensamento e esforço cognitivo. A segunda, no entanto, não requer muita elaboração, e reage quase de forma inconsciente. Por exemplo, fingindo ser uma pessoa com autoridade, como um policial, os infratores podem facilmente obter um nível de obediência das suas vítimas. Estas regras práticas e cognitivas têm os seus usos diários, mas permitem que os infratores as explorem para benefício próprio.

Essas táticas enganosas são usadas numa ampla **variedade de golpes**. *Fraude nigeriana, fraude "granny", fraudes de romance, fraude com CEO* ... as possibilidades são tão infinitas quanto a criatividade dos golpistas. Esta gama de esquemas enganosos permite que os fraudadores atinjam público muito grande de uma só vez ou adotem uma abordagem mais personalizada. Cada vez mais, esta última opção tem vindo a ser utilizada. Os fraudadores aperceberam-se que se selecionassem as suas vítimas com cuidado, o seu "retorno sobre o investimento" se tornava muito mais alto. Os e-mails de phishing estão a tornar-se cada vez mais sofisticados e endereçados a um grupo muito mais pequeno e seletivo. O último e surpreendente passo neste evolução envolve a combinação de novas e mais antigas tecnologias: o telefone. Phishing ou voice phishing fornece a oportunidade de combinar as vantagens da internet e do telefone. Fazendo uma chamada telefónica praticamente sem custos torna mais difícil identificar o autor da chamada. Estas chamadas podem ser automatizadas. O uso do telefone tem vantagens adicionais: as pessoas confiam mais e, graças a uma configuração mais íntima, as vítimas são convencidas mais facilmente. Uma ilustração do nível crescente de sofisticação: os ofensores até contratam falantes nativos para tornar as chamadas telefónicas tão genuínas quanto possível.

Os nossos conhecimentos atuais sobre a fraude individual são, no entanto, bastante limitados. Este crime está rodeado por um grande **desconhecido** pois muitas destas fraudes nunca são relatadas. As vítimas não sabem que foram vitimizadas, não se apercebem da severidade da situação, não pensam que denunciar irá ter algum resultado ou, simplesmente, não sabem

sequer onde apresentar denúncia. Além disso, devido ao papel ativo que a vítima tem na sua própria vitimização, os sentimentos de culpa e vergonha impedem as vítimas de contar as suas histórias. Alguns golpes até têm mecanismos anti-denúncia "integrados", pois as vítimas precisam de realizar ações ilegais no esquema, incriminando-se no processo. Relatar a fraude iria fazer a vítima sentir-se como se se estivesse a auto-incriminar.

Este número desconhecido também deu origem ao **mito** de que os idosos são as vítimas principais deste crime por constituírem um alvo fácil. Alguns estudos refutaram esse mito, embora devamos permanecer cautelosos devido ao facto de as pequisas disponíveis serem muito limitadas. No entanto, a população mais jovem e o grupo médio foram identificados como sendo mais suscetíveis a fraudes. Outro mito que existe é que as vítimas são tipicamente retratadas como não instruídas ou financeiramente inaptas, mas o oposto parece ser verdade. Uma explicação possível é chamada de "lacuna entre o conhecimento e as ações", onde as pessoas conseguem reconhecer os sinais de uma fraude, mas não conseguem aplicar esse conhecimento à sua própria situação.

Infelizmente, a existência das chamadas '**sucker lists**' (ou "listas de vítimas fáceis") não é um mito. Os fraudadores por telefone podem contactar as suas vítimas de modo aleatório ou procurando nas listas telefónicas públicas, mas também partilham entre si listas com alvos que já foram defraudados. O uso de tais listas é indicativo de um alto nível de vitimizações repetidas. Por exemplo, alguns fraudadores irão tentar "ajudar" as suas vítimas a recuperar o que perderam...

Como o policiamento desse crime é extremamente difícil, a necessidade de prevenção é alta. No entanto, foram conduzidas poucas pesquisas académicas e avaliações sobre a fraude individual. Apesar disso, podemos postular algumas conclusões gerais. A tática de prevenção mais comum é a educação do público. Isto pode ser realizado através de uma campanha de conscientização, mas especialmente quando esta informação foi comunicada no âmbito de uma formação, notaram-se efeitos positivos. Basicamente, estas formações tentam diminuir a lacuna entre o conhecimento e as ações, à qual nos referimos anteriormente. Uma outra tática chave é colaborar com as vítimas. Devido ao seu papel ativo e ao risco existente de vitimização repetida, as vítimas deverão ser apoiadas e conscientizadas sobre as suas posições específicas.

Durante a presidência da Bulgária, o secretariado reuniu um número de **boas práticas** sobre este tema. Elas podem ser categorizadas de acordo com o seu grupo alvo. Uma primeira categoria concentra-se na totalidade da população. Trata-se de campanhas de conscientização, como os exemplos da Bulgária, Suécia, Bélgica, ou da Europol. Estas campanhas incluem publicidades na rádio, posteres, brochuras, brindes... que fornecem informações úteis para o público e mostram como se pode proteger contra este tipo de fraude. Um segundo grupo de atividades destina-se ao contacto com os idosos. Aqui, estão a ser implementados métodos mais interativos, como é o caso da República Checa. Os idosos participam numa peça educacional interativa, onde aprendem sobre os esquemas fraudulentos mais comuns e como reagir a eles. Esta "experiência vivida" permite-lhes reagir de forma adequada aos cenários da vida real. A avaliação deste projeto comprovou que esta conclusão é verdadeira, pois o grupo recusou duas vezes e meia mais fraudes do que um grupo de controlo que não assistiu à peça. A última categoria de atividades de prevenção concentra-se nas vítimas. Exemplos da Austrália, Reino Unido e Canadá mostraram a necessidade deste tipo de prevenção. No entanto, existem - mesmo a nível global - poucos serviços de suporte para as vítimas de fraudes individuais.

Finalmente, o secretariado da EUCPN organizou um atelier com diversos peritos para elaborar algumas **recomendações** sobre como prevenir as fraudes telefónicas. Estas recomendações estão estruturadas de acordo com as cinco estratégias de prevenção situacional do crime. A primeira estratégia possível é aumentar o esforço que um infrator tem de fazer para que a fraude tenha sucesso. A restrição da publicação e acesso aos números de telefone pode ajudar neste sentido. Uma outra técnica poderia consistir em limitar a quantidade de números de telefone que uma pessoa pode ter ou, no mínimo, ligá-los a uma conta bancária ou número de identificação.

Uma segunda estratégia é aumentar os riscos. Aqui, é muito importante partilhar informações. Esta partilha não deverá parar nas fronteiras do sector público ou privado, ou a nível nacional. Todos os parceiros têm um papel importante no puzzle das informações. Sabendo com o que está a lidar aumenta as probabilidades de evitar que algo aconteça em primeiro lugar. Escusado será dizer que os relatórios deveriam ser mais fáceis e abordáveis. As informações têm de ser recolhidas antes de poderem ser partilhadas. Foram feitas outras recomendações para diminuir a anonimidade do autor da chamada, tornando praticamente impossível falsificar a localização. O software de reconhecimento de voz também poderia ser interessante.

A diminuição das recompensas que pode ser alcançada cometendo este crime é uma terceira estratégia para evitar as fraudes telefónicas. A apreensão dos ativos obtidos ilegalmente é a principal recomendação neste caso. Neste sentido, monitorar o fluxo de dinheiro é crucial para detetar transações suspeitas. Uma iniciativa com o setor bancário em toda a UE para facilitar esta tarefa foi recomendada pelos nossos especialistas.

Uma outra estratégia é diminuir as provocações. Assim, é importante não partilhar demasiadas informações sobre como a fraude foi executada, para evitar os "copycats". Além disso, esta estratégia pode ajudar a evitar algumas formas de repetição. A estratégia final é eliminar as desculpas. Isto concentra-se principalmente na conscientização sobre a fraude telefónica e sobre como se proteger. As boas práticas de anteriormente estão indicadas como exemplos chave aqui. As campanhas de conscientização deveriam espalhar a mesma mensagem. Por isso é importante implementar parcerias público-privadas e colaborações internacionais para garantir a consciência de que *basta dizer que não.*