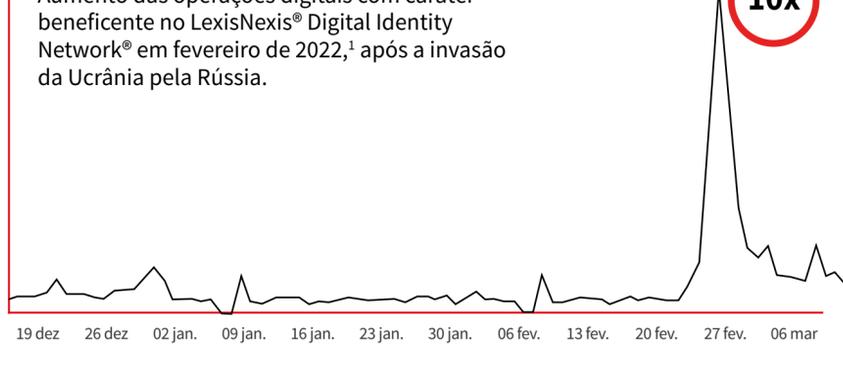


Da mesma maneira que as pessoas agem rápido para doar, os golpistas também se mexem

As crises mundiais, como a pandemia da Covid-19 e os ataques da Rússia contra a Ucrânia, costumam estimular a ação dos cidadãos conscientizados e, infelizmente, dos fraudadores também.

1 | Normalmente, crises mundiais são seguidas por ondas de doações e ações de caridade.

Aumento das operações digitais com caráter beneficente no LexisNexis® Digital Identity Network® em fevereiro de 2022,¹ após a invasão da Ucrânia pela Rússia.



Contribuição do Banco Mundial no combate aos impactos da pandemia:

US\$ 92,5 bilhões

31 de dezembro de 2018 - 31 de março de 2020

US\$ 157 bilhões

1 de abril de 2020 – 30 de junho de 2021²

+60%

Aumento das doações nos 15 meses anteriores à pandemia



+30%

Aumento no número de doações autodeclaradas no Reino Unido ao longo de uma semana de março de 2022.³

2 | Os fraudadores vão atrás do dinheiro.

+569% <http://www.>

Crescimento no número de criminosos registrando domínios com palavras-chave como “coronavírus” e “covid”, de fevereiro a março de 2020.⁴

Isso equivale a 200 mil novos sites registrados em 80 países.



+68%

De denúncias de arrecadações de fundos falsos para vítimas da guerra na Ucrânia recebidas pelo Centro Nacional de Relatórios de Fraudes do Reino Unido até março de 2022.⁵



US\$14 bilhões

Valor dos golpes relacionados a criptomoedas durante a pandemia de Covid 19 em 2021.

3 | Os golpes envolvendo ações de caridade variam em tipo e estratégia.



Golpes de pessoas necessitadas, que alegam urgência e exigem confidencialidade



Golpes por meio de exames, vacinas e tratamento oferecem testes caseiros falsos e curas “milagrosas”



Fraudadores que se passam por instituições de caridade legítimas usando uma lista de pessoas vulneráveis que precisam de apoio, compartilhando um site falso para doações⁷



Fraudes de fornecimento, vendendo de equipamento de proteção individual (EPI) para caridades, como máscaras e luvas

4 | Quatro maneiras de proteger a sua doação.

- 1 Doe diretamente para organizações beneficentes conhecidas.
- 2 Se você nunca ouviu falar da organização, pesquise-a na internet para ver se não há nenhuma acusação de golpes contra ela.⁸
- 3 Se você for contatado diretamente e o contato forçar uma ação imediata com base no emocional, não caia no golpe e faça uma pesquisa antes de solicitar qualquer atitude.
- 4 Desconfie se solicitarem um cartão, ou a aquisição de algum cartão vale-presente.

Para outras dicas, consulte os sites de proteção ao cliente do seu país, como: <https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams>

A LexisNexis® Risk Solutions continua a acompanhar essas tendências associadas a pandemia e a invasão russa da Ucrânia em nosso LexisNexis® Digital Identity Network®

Fique à frente dos golpistas com uma abordagem em camadas contra fraudes.

Veja como a LexisNexis® Risk Solutions reúne gestão de fraudes, verificação de identidade e informações sobre risco utilizando inteligência de rede, cobertura global confiada pelo setor e propriedade intelectual para permitir que a sua empresa diferencie, com confiança, entre um cliente confiável e uma ameaça, ao mesmo tempo em que mantém a experiência do cliente ininterrupta.

<https://risk.lexisnexis.com/global/pt/insights-resources/white-paper/authorized-push-payment-scams>