Segurança da informação em áreas de alto impacto

Por Jarrah Bloomfield e a equipe da 80.000 Hours. Publicado em inglês em dezembro de 2022. Última atualização em junho de 2023·

Traduzido, editado e adaptado pela equipe do Carreiras Eficazes, de modo a atender as necessidades das comunidades lusófonas com autorização dos produtores do texto original.

Conforme a campanha presidencial dos EUA de 2016 entrava em uma rodada turbulenta das primárias, o presidente da campanha de Hillary Clinton, John Podesta, abriu um e-mail perturbador. [1] A mensagem de 19 de março alertava que a sua senha do Gmail havia sido comprometida e que ele precisava alterá-la urgentemente.

O e-mail era uma mentira. Não estava tentando ajudá-lo a proteger a sua conta: era um ataque de phishing tentando ganhar acesso ilícito.

Podesta estava desconfiado, mas a equipe de tecnologia da informação (TI) da campanha escreveu erroneamente que o e-mail era “legítimo” e lhe disse para alterar a sua senha. A equipe de TI forneceu um link seguro para Podesta usar, mas parecia que um dos seus funcionários, em vez disso, clicou no link do e-mail falsificado. Esse link foi usado pelos hackers da inteligência russa conhecidos como “Fancy Bear”, e usaram seu acesso para vazar e-mails privados da campanha para o consumo público nas semanas finais da eleição de 2016, constrangendo a equipe de Clinton.

Embora seja plausível que haja muitos fatores cruciais em qualquer eleição, é possível que a controvérsia em torno dos e-mails vazados tenha tido um papel não trivial na perda subsequente de Clinton para Donald Trump. Isso significa que a falha da equipe de segurança da campanha na prevenção do hackeamento — que poderia ter se resumido a um mero erro de digitação[2] — foi extraordinariamente significativa.

Esses eventos ilustram vividamente como carreiras em segurança da informação em organizações cruciais têm o potencial de impacto descomunal. Idealmente, os profissionais de segurança podem desenvolver práticas robustas que reduzam a probabilidade de que um único deslize resulte em uma violação significativa. Mas esse componente essencial para o funcionamento prolongado e preservado de organizações importantes é muitas vezes negligenciado.

E a necessidade de tal proteção se estende para bem além do caso de hackers tentarem causar o caos em época de eleição. A segurança da informação é essencial para proteger todos os tipos de organizações cruciais, como aquelas que armazenam dados extremamente sensíveis sobre ameaças biológicas, armas nucleares ou inteligência artificial avançada, que poderiam ser alvos de hackers criminosos ou nações agressivas. Tais ataques, se bem-sucedidos, poderiam contribuir para dinâmicas competitivas perigosas (como corridas armamentistas) ou levar diretamente a uma catástrofe.

Algumas funções em segurança da informação envolvem a gestão e coordenação de políticas organizacionais, o trabalho em aspectos técnicos da segurança ou uma combinação de ambos. Cremos que muitas dessas funções até o momento foram subestimadas entre aqueles interessados no altruísmo eficaz e na redução de riscos globais catastróficos e estaríamos animados em ver candidatos com motivações altruístas mudarem para este campo.

Em resumo: organizações com influência, poder financeiro e tecnologias avançadas são alvos de atores que buscam roubar ou abusar desses recursos. Uma carreira em segurança da informação é um caminho promissor para apoiar organizações de alto impacto na proteção a esses ataques, que têm o potencial de perturbar a missão de uma organização ou até aumentar o risco existencial.

Recomendado

Se você for apto para esta carreira, ela pode ser a melhor maneira para você ter um impacto social.

Status da análise

Baseada em uma investigação de profundidade média.

(Esta análise é informada por pessoas com especialidade sobre este caminho, um entendimento sobre os melhores conselhos existentes e uma investigação aprofundada sobre pelo menos uma das nossas incertezas fundamentais referentes a este caminho. Algumas das nossas opiniões serão pesquisadas minuciosamente, embora seja provável que permaneçam algumas lacunas no nosso entendimento.)

Jeffrey Ladish contribuiu para esta análise de carreira. Também agradecemos a Wim van der Schoot pelos seus comentários úteis.

Por que a segurança da informação poderia ser uma carreira de alto impacto?

A segurança da informação protege uma organização de eventos que prejudicam a sua capacidade de cumprir a sua missão, como invasores ganhando acesso a informações confidenciais. Especialistas em segurança da informação têm um papel essencial em apoiar a missão de organizações, similar a funções em operações.

Logo, se você deseja ter uma carreira impactante, o conhecimento em segurança da informação poderia capacitar você a fazer uma diferença positiva considerável no mundo, ao ajudar organizações e instituições importantes a serem seguras e bem sucedidas.

Em comparação com outras funções em tecnologia, uma carreira em segurança da informação pode ser uma opção segura, porque há menos risco de ter um impacto negativo. Em geral, prevenir ataques torna o mundo um lugar melhor, ainda que não seja claro se as próprias organizações que são vítimas potenciais, estão proporcionando um impacto mais positivo do que negativo. Quando uma empresa é hackeada, o dano pode cair desproporcionalmente sobre os outros, como pessoas que confiaram na empresa com as suas informações privadas.

Por outro lado, funções em segurança da informação às vezes têm um impacto limitado, mesmo quando apoiam áreas de alto impacto, se a organização não valoriza genuinamente a segurança. Muitas organizações têm funções de segurança principalmente para que possam cumprir as normas e os padrões de conformidade para fazer negócios. Essas padrões de segurança têm um papel importante, mas quando são aplicadas sem a preocupação de obter resultados de segurança reais, muitas vezes isso leva a um teatro de segurança. Não é comum para profissionais de segurança darem-se conta de que estão tendo um impacto mínimo na postura de segurança da sua organização.

Proteger organizações que trabalham nos problemas mais urgentes

Organizações que trabalham em problemas urgentes precisam de conhecimento em segurança cibernética para proteger seus sistemas de computador, recursos financeiros e informações confidenciais de ataques. De certa forma , esses desafios são semelhantes àqueles encarados por outras organizações; no entanto, organizações que trabalham em grandes problemas são às vezes alvos especiais de ataques.

Essas organizações — como aquelas que estão tentando monitorar patógenos perigosos ou coordenar a redução de tensões globais — muitas vezes trabalham com instituições internacionais, autoridades políticas locais e governos. Elas podem ser alvos de ataques

patrocinados por países com interesses geopolíticos relevantes, tanto para roubar informações, quanto para ganhar acesso a outros alvos de alto valor.

Algumas organizações de alto impacto têm discussões confidenciais e sensíveis como parte do seu trabalho, nas quais um vazamento de informação por meio de um comprometimento de segurança, prejudicaria a confiança e a capacidade de cumprir sua missão. Isso é especialmente relevante ao operar em países com regimes de controle de informações e censura.

Além de ameaças de invasores patrocinados por Estados, grupos de crimes cibernéticos também criam sérios riscos.

Eles buscam o ganho financeiro, por meio da extorsão e da fraude: por exemplo, modificando informações de pagamento, resgatando dados ou ameaçando vazar correspondências confidenciais. Qualquer organização é vulnerável a esses ataques. Mas organizações que lidam com informações particularmente sensíveis ou transações financeiras de grande valor, como fundos de financiamento filantrópicos, são alvos especialmente prováveis.

Em casos extremos, algumas organizações precisam de ajuda para proteger informações que poderiam ser nocivas para o mundo se fossem conhecidas de forma mais ampla, como sequências genéticas ou tecnologias de IA poderosas.

A segurança de sistemas de IA avançados

Embora acreditemos que a segurança da informação possa ser valiosa em muitas organizações de alto impacto, proteger os sistemas de IA mais avançados pode estar entre os trabalhos de maior impacto que você poderia fazer.

Atualmente classificamos os riscos da inteligência artificial como o problema mais urgente do mundo, devido ao potencial para sistemas futuros causarem catástrofes em uma escala global. E para reduzir o risco de uma catástrofe relacionada à IA, recomendamos que algumas pessoas trabalhem no campo da segurança da IA.

Mas ainda que as empresas que estão desenvolvendo modelos de IA os utilizem com responsabilidade e de acordo com altos padrões de segurança, esses esforços poderiam ser comprometidos se um ator externo roubar a tecnologia e então implementá-la de forma irresponsável. E porque é esperado que os modelos de IA avançados sejam poderosos e economicamente valiosos ao extremo, há atores tanto com um interesse em roubá-los quanto com um histórico de lançar ataques cibernéticos bem-sucedidos para roubar tecnologias.

Como a segurança da informação é uma habilidade altamente procurada, algumas organizações relacionadas à IA descobriram que é difícil contratar para essas funções cruciais. Poderia haver também uma demanda especial por pessoas que entendam os desafios especiais de segurança da informação relacionados à IA; trabalhar neste tópico poderia ter um alto impacto e fazer de você um candidato de emprego desejável.

Como efetivamente é trabalhar em funções de segurança da informação de alto impacto?

Funções "defensivas" em segurança cibernética — nas quais o principal trabalho é a defesa de ataques de pessoas de fora — são aquelas cuja demanda é a mais comum, especialmente em organizações sem fins lucrativos menores e startups de mentalidade altruísta, que não têm os recursos para contratar um único especialista em segurança.

Em algumas dessas funções, você se encontrará fazendo uma mistura de trabalho técnico prático e comunicando o risco de segurança. Por exemplo:

- Você aplicará um entendimento sobre como os hackers trabalham e como detê-los.
- Você estabelecerá sistemas de segurança, analisará configurações de TI e fornecerá conselhos para a equipe, sobre como fazer seu trabalho com segurança.
- Você fará testes em busca de erros e vulnerabilidades e projetará sistemas e políticas que sejam robustos para uma gama de ataques possíveis.

Ter conhecimento sobre segurança em uma ampla gama de temas de TI organizacional ajudará você a ser mais útil, como segurança de notebook, administração de nuvem, segurança de aplicativos e contas de TI (com frequência chamadas de "gestão de identidade e acesso").

Você pode ter um impacto descomunal em comparação a outra contração potencial, trabalhando para uma organização de alto impacto, onde você compreenda a área de causa dela. Isso ocorre porque a segurança da informação pode ser desafiadora para organizações que focam no impacto social, visto que conselhos em segurança cibernética de normas industriais são criados para apoiar motivações orientadas ao lucro e estruturas regulatórias. **Adaptar a cibersegurança ao modo como uma organização está tentando alcançar a sua missão — e para evitar os eventos nocivos que mais importam à organização — poderia aumentar muito sua eficácia.**

Se você está interessado em reduzir riscos existenciais, achamos que deveria considerar juntar-se a uma organização que trabalha em áreas relevantes, como inteligência artificial, conforme discutido acima, ou biorrisco.

Uma parte importante disso é trazer a sua equipe para a jornada. Para fazer segurança bem, você estará pedindo com frequência às pessoas para mudar o modo como elas trabalham (provavelmente acrescentando obstáculos!), de modo que ser um comunicador eficaz pode ser tão importante quanto entender os detalhes técnicos. Ajudar todos a entender por que certas medidas de segurança importam e como você está equilibrando os custos e benefícios, é necessário para a equipe aceitar um esforço a mais ou passos aparentemente desnecessários.

Funções de hackeamento ético, nas quais você recebe a tarefa de quebrar as defesas dos seus clientes ou empregados a fim de, em última análise, melhorá-las, são também importantes para a segurança cibernética — mas só organizações muito grandes têm posições para esses tipos de funções "ofensivas" (ou de "equipe vermelha"). Com mais frequência, tais funções estão em empresas de serviços de segurança cibernética, que são pagas para fazer exercícios de teste de penetração de curto prazo para clientes.

Se você conseguir uma função dessas, seria difícil focar na segurança de organizações impactantes a fim de maximizar o seu impacto, pois você muitas vezes têm pouca escolha sobre quais clientes está apoiando. Mas você teria o potencial de construir capital de carreira nesses tipos de funções, antes de mudar para empregos mais impactantes.

Que tipo de salários ganham os profissionais em segurança cibernética?

Os profissionais em funções de segurança da informação, como segurança cibernética, ganham altos salários. A Agência dos EUA de Estatística do Trabalho reportou que o salário mediano para analistas de segurança da informação era de mais de US$ 100.000 por ano em 2021. Em algumas funções, como aquelas nas melhores empresas de IA, os candidatos certos podem ganhar até US$ 500.000 por ano ou mais.

Embora seja provável que você tenha um maior impacto apoiando uma organização diretamente, se a organização estiver fazendo um trabalho particularmente importante, ganhar para doar ainda pode ser uma opção de alto impacto, especialmente quando você foca em doar para os projetos mais eficazes que poderiam usar os fundos extras.

Como avaliar a sua adequação com antecedência?

Uma ótima maneira de avaliar a sua adequação para a segurança da informação é experimentá-la. Há muitos recursos online gratuitos que podem ensinar você o básico ou te dar uma experiência prática com aspectos técnicos da segurança.

Você pode ter uma introdução por meio do curso Fundamentos da Cibersegurança do Google, que você pode assistir de graça se selecionar a opção “audit” no canto inferior esquerdo no menu de inscrição. A série completa do Certificado Profissional de Cibersegurança do Google também vale a pena assistir para aprender mais sobre temas técnicos relevantes.

Algumas outras ideias para começar:

- **Experimente hacking ético para entender como os hacks funcionam e desenvolva uma intuição sobre vulnerabilidades de segurança.** Encontre um tutorial sobre ataques básicos (por exemplo, OverTheWire, HackTheBox) ou um curso (por exemplo, Ethical Hacking Essentials da Coursera). Leia sobre vulnerabilidades relevantes e veja se há guias sobre como configurar um ambiente de laboratório e explorá-las (por exemplo, Log4Shell). Se você estiver estudando em uma universidade, pode ser fácil se juntar a uma equipe de Capture the Flag (CTF).
- **Brinque com ferramentas de segurança.** O Wireshark irá inspecionar a surpreendente variedade de tráfego de rede no seu computador, e a Burp Suite Community pode ir mais fundo em solicitações da web. Faça uma varredura da sua rede doméstica para encontrar vulnerabilidades com o Nessus Essentials.
- **Monte a sua própria infraestrutura.** Hospede uma máquina virtual. Construa um servidor da web e proteja-o. Tente instalar o Elastic Stack e o Zeek. Consiga o AWS Free Tier e examine as configurações do administrador da nuvem.

Ter habilidade para descobrir como sistemas de computador funcionam ou gostar de empregar uma mentalidade de segurança são indicadores de que você pode ser adequado, mas não são necessários para começar na segurança da informação.

Como ingressar na segurança da informação

Ingressar com um diploma

O modo tradicional de ingressar neste campo é estudar uma disciplina de TI — como ciência da computação, engenharia de software, engenharia de computadores ou um campo relacionado — em uma universidade que tenha uma boa gama de cursos de segurança cibernética. No entanto, você não deve pensar que isso é um pré-requisito: **há muitos praticantes de segurança bem-sucedidos sem um diploma formal.** No entanto, um diploma muitas vezes facilita conseguir empregos de iniciante, porque muitas organizações ainda o requerem.

Além dos cursos classificados como cibersegurança, um bom entendimento dos fundamentos dos sistemas de computador é útil. Isso inclui tópicos sobre redes de computadores, sistemas operacionais e o básico de como o hardware de computadores funciona. Sugerimos que você considere pelo menos um curso de aprendizado de máquina: embora seja difícil prever as mudanças tecnológicas, é plausível que as tecnologias de IA venham a mudar dramaticamente o panorama da segurança.

Considere encontrar um emprego de meio período em uma área de TI, enquanto estuda (veja a próxima seção), ou fazer um estágio. Isso não precisa ser em uma função de segurança da informação; pode simplesmente ser uma função na qual você tem a oportunidade de ver em primeira mão como a TI funciona. O que você aprende na universidade e o que acontece na prática são coisas diferentes, e entender como a TI é aplicada no mundo real é essencial.

No último ano da sua formação universitária, procure posições iniciantes em segurança cibernética, ou outras posições em TI, caso precise.

Acreditamos que empregos em funções defensivas em segurança cibernética são ideais para adquirir a ampla gama de habilidades que provavelmente são mais relevantes para organizações de alto impacto. Elas têm cargos como *Analista de Segurança, Operações de Segurança, Diretor de Segurança de TI, Engenheiro de Segurança* ou até *Engenheiro de Segurança de Aplicativos*. Funções “ofensivas” como testagem de penetração também podem fornecer experiências valiosas, mas você pode não ter uma visão geral tão ampla de todas as fontes relevantes para a segurança empresarial, ou vivenciar os desafios com a implementação em primeira mão.

Ingressar com (apenas) experiência em TI

Também é possível ingressar neste campo sem um diploma.

Se você tem um bom conhecimento operacional de TI ou habilidades de codificação, um caminho comum é começar em uma função júnior em apoio de TI interno (ou em posições semelhantes em serviços de recepção ou assistência técnica) ou relacionada a software. Muitas pessoas que trabalham em segurança cibernética hoje, fizeram uma transição a partir de outras funções em TI. Isso pode funcionar bem, se você está interessado especialmente em computadores e está motivado a mexer com sistemas de computador no seu tempo livre.

Muito do que você aprenderá em uma função organizacional de TI, será útil para funções de cibersegurança. Uma gestão de TI sólida requer segurança cotidiana, e entender como os

sistemas funcionam e os desafios causados pelos recursos de segurança, é importante para você ser eficaz na segurança cibernética.

Você precisa de certificados?

Há muitos certificados de segurança cibernética que você pode conseguir. Eles não são obrigatórios, mas ter um pode te ajudar a conseguir um emprego de nível iniciante, especialmente se você não tiver um diploma. A utilidade varia de acordo com a reputação do provedor, e o treinamento e os exames podem ser caros.

Alguns certificados bem conceituados são o CompTIA Security+, o GIAC Security Essentials, o OSCP Penetration Testing e o Certified Ethical Hacker. Certificados de fornecedores e de tecnologia (p. ex., Microsoft ou AWS) geralmente não são valiosos a não ser que sejam específicos para um emprego que você está buscando.

Em que tipos de lugar você deveria trabalhar?

Para os seus primeiros anos, recomendamos priorizar a descoberta de uma função que aumentará o seu conhecimento e capacidade rápido. Algumas organizações de alto impacto são bem pequenas, de modo que elas podem não estar bem posicionadas para treinar você no início da sua carreira, pois provavelmente têm menos capacidade de orientação em uma gama de áreas técnicas.

Encontre um emprego no qual você possa aprender boa TI ou gestão de segurança cibernética com outras pessoas.

Os melhores lugares onde você pode trabalhar, já têm práticas de gestão de segurança e maturidade organizacional relativamente boas, de modo que você pode ver como as coisas devem ser. Você também pode ter uma noção sobre as barreiras que impedem as organizações de terem práticas de segurança *ideais*. Ser capaz de fazer perguntas a profissionais experientes e descobrir o que é efetivamente viável, ajuda você a aprender mais rápido, do que você mesmo correr contra todas as barreiras.

As empresas de tecnologia e as organizações financeiras têm uma reputação mais forte para a segurança cibernética. Organizações especialistas em segurança — como em consultoria, fornecedores de segurança gerenciados ou empresas de software de segurança — podem ser ótimos lugares para aprender. Organizações governamentais que se especializam em segurança cibernética podem fornecer experiência valiosa, que é difícil de conseguir fora de funções específicas.

Quando tiver melhorado as suas habilidades, a principal coisa a procurar é um lugar que esteja fazendo trabalhos importantes. Pode ser uma agência do governo, uma organização sem fins lucrativos ou até uma organização com fins lucrativos. Listamos algumas organizações de alto impacto aqui. A segurança da informação é uma função de apoio necessária em todas as organizações em diferentes níveis. **O quanto seu impacto é positivo, dependerá muito do fato de você estar projetando uma organização que faça um trabalho importante e urgente.** Abaixo discutimos áreas específicas nas quais acreditamos que mais pessoas poderiam fazer um trabalho mais impactante.

Proteger os riscos da informação

Proteger informações que poderiam ser prejudiciais para o mundo caso fossem roubadas, pode ser especialmente impactante e poderia ajudar a diminuir o risco existencial.

Algumas informações poderiam aumentar o risco de que a humanidade se torne extinta, caso fossem vazadas. Organizações focadas na redução desse risco podem precisar criar ou usar essas informações como parte do seu trabalho, de modo que trabalhar emsua segurança, significa que você pode ter um impacto diretamente positivo. Exemplos incluem:

- Empresas e laboratórios de IA, conforme discutido acima, que podem descobrir tecnologias que poderiam causar danos à humanidade nas mãos erradas.
- Pesquisadores em biorrisco que trabalham com materiais sensíveis, como sequências genéticas nocivas que poderiam ser usadas para projetar pandemias
- Fundações de pesquisa e concessão de financiamento, que têm acesso a informações sensíveis sobre as estratégias e resultados de organizações de redução de risco existencial

Contribuir para a IA segura

Habilidades de segurança são relevantes para prevenir uma catástrofe relacionada à IA. Profissionais de segurança podem trazer uma mentalidade de segurança e habilidades técnicas que possam mitigar o risco de uma IA avançada levar ao desastre.

Se a IA avançada acabar transformando radicalmente a economia global, como alguns creem que pode, o panorama da segurança e a natureza das ameaças discutidas neste artigo, poderiam mudar de formas inesperadas. Entender usos de ponta da IA, tanto por hackers maliciosos, quanto por profissionais de segurança da informação, pode permitir que você tenha um grande impacto, ao ajudar a garantir que o mundo seja protegido de ameaças catastróficas de grande porte.

Trabalhar em governos

Os governos também mantêm informações que poderiam impactar negativamente a estabilidade geopolítica caso fossem roubadas, como tecnologias de armamentos e segredos diplomáticos. Mas pode ser mais difícil ter um impacto positivo por meio deste caminho ao trabalhar no governo, visto que burocracias estabelecidas são muitas vezes resistentes à mudança e essa resistência pode impedir que você tenha um impacto.

Apesar disso, a escala do governo também implica que, se você *for* capaz de fazer uma mudança positiva em áreas impactantes, isso tem o potencial para efeitos de longo alcance.

Pessoas que trabalham nesta área devem reavaliar regularmente se o seu trabalho está fazendo uma diferença significativa, ou se está no caminho para fazê-la. Pode haver melhores oportunidades dentro ou fora do governo.

Você poderia ter um impacto positivo ao trabalhar em segurança cibernética para as agências de segurança nacional do seu país, ou como empregado direto, ou como contratado do governo. Além disso, essas funções podem te dar a experiência e contatos profissionais necessários, para trabalhar de forma eficaz em políticas nacionais de segurança cibernética.

Se você tiver a oportunidade, trabalhar para definir e aplicar políticas de segurança cibernéticas sensatas poderia ser altamente impactante.

Quer conselhos individualizados sobre seguir este caminho?

Se você acha que este caminho pode ser uma grande opção para você, mas precisa de ajuda para decidir ou pensar sobre o que fazer em seguida, a nossa equipe pode ser capaz de ajudar.

Podemos ajudar você a comparar as suas opções, fazer conexões e possivelmente até ajudar você a encontrar empregos e oportunidades de financiamento.

CANDIDATE-SE PARA FALAR COM A NOSSA EQUIPE

Saiba mais

- Relatório de pesquisa: Securing AI Model Weights: Preventing Theft and Misuse of Frontier Models by RAND
- Coleção: Uma lista de organizações de segurança da informação, mantida por nosso quadro de empregos

- Podcast: Sella Nevo sobre quem está tentando roubar modelos de IA de fronteira e o que poderiam fazer com eles
- Podcast: Nova DasSarma sobre por que a segurança da informação pode ser crucial para o desenvolvimento seguro de sistemas de IA
- Podcast: Lennart Heim sobre a era da governança computacional e o que tem de vir depois
- Mitigar biorriscos catastróficos: uma palestra do professor do MIT Kevin Esvelt sobre por que a segurança da informação avançada é importante para reduzir biorriscos
- Considerações de segurança da informação para a IA e o futuro de longo prazo: um post do Effective Altruism Forum de Jeffrey Ladish e Lennart Heim
- Podcast: Bruce Schneier sobre como o voto eletrônico inseguro poderia quebrar os EUA — e a vigilância sem tirania
- Mentalidade de Segurança e Paranoia Corriqueira: uma análise de Eliezer Yudkowsky do Machine Intelligence Research Institute
- OK, então eu Preciso de Segurança. Onde eu Começo?: um artigo de Lyde Andrews do SANS
- Como construir uma carreira de segurança cibernética: um post de Daniel Miessler, um profissional de segurança da informação com mais de 20 anos de experiência
- Carreiras em segurança da informação para a redução de riscos catastróficos globais: um post do Effective Altruism Forum de Claire Zabel e Luke Muehlhauser da Open Philanthropy
- Recursos de políticas, grupos de pesquisa e bolsas de cibersegurança dos EUA

Notas e referências

1. Esse relato se baseia numa reportagem pública do incidente em veículos de notícias que incluem a Vox, a Vice e a CNN.
2. "'Este é um e-mail legítimo', Charles Delavan, um auxiliar de campanha de Clinton, respondeu a outro auxiliar do Sr. Podesta, que havia percebido o alerta. John precisa mudar a sua senha imediatamente.' Com outro clique, uma década de e-mails que o Sr. Podesta mantinha na sua conta do Gmail — um total de cerca de 60.000 — foram desbloqueados para os hackers russos. O Sr. Delavan, em uma entrevista, disse que seu mau conselho foi resultado de um erro de digitação: ele sabia que era um ataque de phishing, visto que a campanha estava recebendo dezenas deles. Ele disse que queria digitar que era um e-mail "ilegítimo", um erro que disse que o atormenta desde então." Veja *The New York Times*.