O que você vai ler:

Resumo

- Os cibercriminosos que enganam as pessoas para que se enganem aumentaram 614% no terceiro trimestre de 2024.
- Cuidado com CAPTCHAs falsos, tutoriais obscuros e golpes de “solução rápida”.
- Fique seguro verificando links, sendo cauteloso ao instalar software e mantendo seu sistema atualizado.

A pior parte de alguns golpes reside na capacidade de se disfarçarem como tarefas inofensivas. Mas como você os identifica e se protege?

Os cibercriminosos estão enganando as pessoas para que elas mesmas se enganem

Quando você pensa em um cibercriminoso ou hacker, você pode pensar em um software de hacking sofisticado sendo usado para invadir suas contas ou em um phisher (um golpista de e-mail) fingindo ser o Príncipe da Nigéria. No entanto, existem outras maneiras pelas quais os cibercriminosos atacam as vítimas: fazendo com que elas se auto-enganem.

Às vezes, o golpe envolve inserir detalhes em uma página de phishing. Outras vezes, é copiar e colar código malicioso na linha de comando. Alguns criminosos vão além e pressionam pessoas inocentes a executar scripts que comprometem seus sistemas e informações confidenciais. Esses truques de engenharia social dispararam impressionantes 614% no terceiro trimestre de 2024, de acordo com a Gen Digital.

CAPTCHAs maliciosos

CAPTCHAs são projetados para proteger contra spam. Os hackers podem ajustá-los para incluir scripts subjacentes que roubam informações. Você pode ver um quebra-cabeça com letras embaralhadas ou uma série de testes baseados em imagens – selecione todos os quadrados com semáforos, por exemplo. Nada parece suspeito superficialmente.

Você pode passar por essa etapa e clicar no botão que baixa uma carga oculta ou concede aos invasores acesso a uma conta. Essas páginas maliciosas às vezes refletem designs de aparência oficial. Eles reproduzem a marca e a linguagem de um serviço estabelecido, combinando perfeitamente com a navegação normal.

Um CAPTCHA legítimo nunca solicitará que você baixe nada ou forneça permissões incomuns.

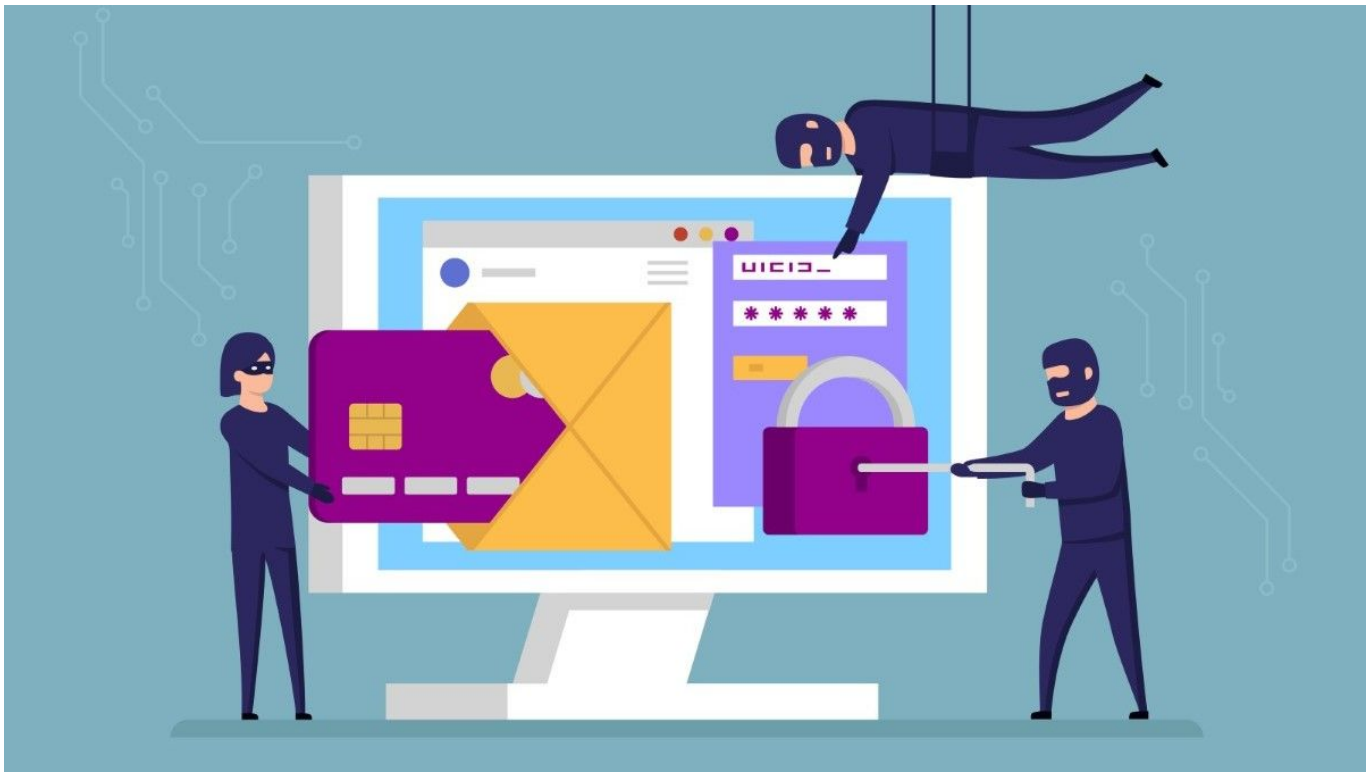
Tutoriais falsos do YouTube

Certos tutoriais em plataformas de vídeo também apresentam perigos ocultos. As instruções prometem resolver um problema frustrante e podem parecer legítimas à primeira vista, com um narrador orientando você em cada etapa. Em algum lugar do vídeo, as instruções aconselham a execução de um script como administrador. A fonte do script está escondida atrás de um link abreviado ou trecho de código na descrição do vídeo. Um pequeno detalhe pode se destacar apenas por um momento, mas o ambiente parece amigável o suficiente para que você decida confiar nele.

O hacker depende desse momento fugaz de credulidade para executar código malicioso em seu sistema. Uma vez executado, pode levar ao roubo de credenciais e comprometer o seu sistema. Tenha cuidado com tutoriais que tenham comentários desativados ou comentários que pareçam spam. Se o vídeo for postado por contas desconhecidas ou novas com poucos vídeos, tome cuidado.

Golpes ClickFix

Você pode ver um e-mail ou pop-up avisando sobre uma falha crítica de segurança e afirmando que um simples clique em um link corrigirá tudo. Por trás disso está uma carga prejudicial que instala spyware, registra as teclas digitadas ou rouba tokens de autenticação. Sua intenção pode ser corrigir um suposto bug, mas o resultado real envolve entregar o controle a um hacker. Se você vir avisos inesperados em pop-ups ou e-mails do navegador, feche a guia ou e-mail e relate imediatamente. Não clique em nenhum link.



Atualizações falsas

Atualizações falsas compartilham o mesmo tema. Chega uma notificação de que seu antivírus (que talvez você nem tenha instalado em seu computador) precisa de uma

atualização urgente. A mensagem urgente pode indicar que está bloqueando uma grande ameaça. Um usuário que deseja tranquilidade clica e segue as instruções. O processo termina e o sistema é reiniciado, só que agora está comprometido. O software que se disfarça como uma atualização de antivírus pode prejudicar suas verdadeiras ferramentas de proteção nos bastidores.

Os hackers gostam desse método porque aproveitam seu desejo de se manter atualizados e seguros. Atualize software apenas de fontes oficiais ou das ferramentas integradas do seu dispositivo – nunca confie em pop-ups aleatórios, e-mails ou sites incompletos.

Como se proteger

Apesar de quantas maneiras diferentes os golpistas e hackers podem atacar você, algumas salvaguardas fáceis evitarão a maioria dos problemas que você possa encontrar.

Verificando URLs

Às vezes parece uma tarefa árdua confirmar a autenticidade de um site ou verificar a legitimidade de um download. No entanto, verificar URLs é fundamental. Identificar um sufixo de domínio estranho ou um subdomínio inesperado pode valer a pena. Se o link afirma levar a um site conhecido, mas o nome de domínio contém letras extras ou pontuação suspeita, é aconselhável recuar. Os cibercriminosos costumam clonar grandes marcas ou portais de serviços, modificando ligeiramente o nome de domínio, esperando que você não perceba.

Lucas Gouveia / How-To Geek | Irina Strelnikova/Shutterstock

Não execute comandos ou scripts aleatórios

Copiar e colar comandos de tutoriais online merece cuidado extra. É tentador pegar o código de um fórum ou vídeo do YouTube e colá-lo diretamente no terminal ou no prompt de comando. Verifique cada linha antes de pressionar Enter. Tenha cuidado com comandos executados com privilégios elevados – procure o comando no Google, se necessário. Também recomendo não executar scripts como administrador ou usuário root, pois a probabilidade de malware em seu sistema é alta.

Tenha cuidado de onde você instala o software

Instalar software de editores desconhecidos sempre será arriscado. Baixar qualquer coisa de links aleatórios ou sites suspeitos pode causar problemas de segurança. Lojas oficiais de aplicativos, sites de fornecedores ou repositórios de software confiáveis são apostas mais seguras. Nunca há garantia de proteção absoluta, mas pelo menos as plataformas amplamente utilizadas possuem alguma triagem de segurança. Sites sem marca prometem conveniência ou afirmam hospedar downloads gratuitos de ferramentas caras. Mesmo que o software funcione, ele pode ocultar surpresas extras que rastreiam, exploram ou sabotam seu sistema.

Use privilégios de não administrador

Executar seu sistema com privilégios de não administrador sempre que possível também oferece um ambiente mais seguro. Muitas tarefas rotineiras não requerem acesso elevado. Se você estiver apenas navegando na internet, enviando e-mails ou editando documentos, um perfil de usuário padrão é suficiente. Os ataques que dependem de direitos de administrador não funcionam se a sua conta não conceder esse nível de poder. Você poderá ver um prompt solicitando uma senha ou avisando que uma ação requer privilégios mais elevados. Reservar um momento para negar privilégios extras pode protegê-lo de permitir que algo perigoso seja executado.

Mantenha seu sistema e programas atualizados

Manter o software atualizado continua sendo essencial para a segurança cibernética. Os fornecedores corrigem vulnerabilidades assim que tomam conhecimento delas. Os invasores monitoram o ciclo de patches. No instante em que percebem um produto amplamente utilizado com uma falha recém-revelada, eles criam uma exploração que tem como alvo os usuários que ainda não atualizaram. Atrasar uma atualização tem seus riscos e é importante instalar patches críticos para ficar à frente desses hackers.

Os invasores normalmente usam engenharia social para contornar defesas sofisticadas e firewalls sofisticados. O elemento humano continua a ser o componente mais arriscado em qualquer cadeia de segurança. As pessoas querem confiar nos outros ou resolver problemas rapidamente. Os criminosos se alimentam dessa empatia ou urgência. Confie nos seus instintos quando sentir que algo não está certo e mantenha-se informado.