FBI alerta público sobre site IC3 falsificado usado em esquemas de fraude

Data: 2025-09-22 13:57:42

Autor: Inteligência Against Invaders

FBI alerta público sobre site IC3 falsificado usado em esquemas de fraude

O FBI alerta que os criminosos estão falsificando o site IC3 para roubar dados pessoais e cometer fraudes contra repórteres de crimes cibernéticos.

O FBI alertou que os invasores estão falsificando o site oficial do Crime Complaint Center (IC3) para roubar dados pessoais e cometer fraudes financeiras, visando usuários que denunciam crimes cibernéticos.

Os sites falsos imitam o domínio IC3 real usando pequenas alterações na ortografia ou nos domínios de nível superior, induzindo os usuários a enviar detalhes confidenciais, como nomes, endereços, e-mails e informações bancárias. As vítimas podem, sem saber, acessar esses sites enquanto tentam registrar reclamações de crimes cibernéticos, expondo-as a fraudes e golpes. A agência pede ao público que verifique os URLs com cuidado ao acessar os serviços do IC3.

“O Federal Bureau of Investigation (FBI) está fornecendo este Anúncio de Serviço Público (PSA) para alertar que os agentes de ameaças estão falsificando o site do governo do FBI Internet Crime Complaint Center (IC3).” lê o Anúncio de serviço público do FBI*“Os agentes de ameaças criam sites falsificados, muitas vezes alterando ligeiramente as características dos domínios legítimos do site, com o objetivo de coletar informações de identificação pessoal inseridas por um usuário no site, incluindo nome, endereço residencial, número de telefone, endereço de e-mail e informações bancárias.”*

O Internet Crime Complaint Center (IC3) é uma parceria entre o FBI e o National White Collar Crime Center (NW3C). Ele serve como a principal plataforma nos EUA para denunciar crimes cibernéticos e fraudes relacionadas à Internet.

O FBI aconselha os usuários a serem cautelosos ao acessar o site do Internet Crime Complaint Center (IC3). Para se manterem seguros, eles devem digitar www.ic3.gov diretamente em seu navegador, em vez de depender de mecanismos de pesquisa, já que os resultados patrocinados geralmente levam a sites fraudulentos. É essencial verificar se o URL termina em **.Gov** e evitar clicar em links suspeitos ou imitações de baixa qualidade. Os usuários nunca devem compartilhar informações confidenciais, a menos que tenham certeza da legitimidade do site. É importante ressaltar que o IC3 não pede pagamentos, não faz parceria com empresas para recuperar fundos perdidos e não possui contas de mídia social.

“O FBI solicita que as vítimas em potencial relatem quaisquer interações com sites ou indivíduos que

se passem pelo IC3 ao escritório local do FBI ou ao IC3 emwww.ic3.gov“, conclui o PSA.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,FBI)