Os sofisticados hacks de phishing dos cibercriminosos. Como os golpistas exploram a tecnologia de acesso remoto seguro



O phishing é uma das principais preocupações de segurança entre empresas e particulares. Com o aumento dos ataques cibernéticos, os incidentes de phishing aumentaram constantemente nos últimos anos. Em 2021, o phishing foi o crime cibernético mais relatado nos EUA, de acordo com uma pesquisa realizada pela Statista, e a principal causa de mais de 50% das infecções de ransomware em todo o mundo em 2020. Para as empresas, ser vítima de ataques de phishing pode se tornar muito caro, pois o perda de credibilidade entre clientes e parceiros pode estar em jogo.

Embora o e-mail ainda seja a ferramenta mais comum usada para phishing, os cibercriminosos intensificaram seu jogo, usando métodos mais sofisticados. Suas técnicas vão além do envio de e-mails e incluem estratégias inteligentes de engenharia social que às vezes são difíceis de expor. O

objetivo dos ataques de phishing é roubar dados confidenciais, como informações bancárias e detalhes de cartão de crédito, ou cometer roubo de identidade obtendo acesso a contas online ou assumindo o controle de computadores inteiros.

Felizmente, você não está completamente indefeso contra fraudadores online. Certas estratégias e truques ajudarão você a proteger seus dados. Reconhecer uma tentativa de phishing quando ela acontece é fundamental para garantir que suas informações não sejam roubadas.

Como os golpistas exploram a tecnologia de acesso remoto seguro

O phishing em si não é um fenômeno novo. Ela existe desde o uso comercial da internet. A tecnologia está em constante evolução, assim como os métodos dos cibercriminosos. Um mundo digital e interconectado facilita o acesso de fraudadores a informações confidenciais.

Infelizmente, houve casos em que os golpistas abusaram da Tecnologia de Acesso Remoto como uma ferramenta potencial para aumentar suas tentativas de phishing. Com esse uso indevido, eles criam a ilusão de que a Tecnologia de Acesso Remoto não seria segura. As soluções profissionais de área de trabalho remota, no entanto, são ferramentas seguras para acessar dispositivos remotamente. Para as empresas, a Tecnologia de Acesso Remoto traz muitas vantagens. Ele permite que os empregadores ofereçam trabalho remoto a seus funcionários e oferece aos departamentos de TI a base certa para um excelente suporte e administração de TI.

É importante entender que esse tipo de software é feito para atender até mesmo às diretrizes de segurança mais rígidas. As Ferramentas de Área de Trabalho Remota criptografam todos os dados e oferecem os mais altos padrões de segurança para manter todas as conexões de entrada e saída protegidas de olhares indiscretos. Permitir que um cibercriminoso acesse remotamente seu dispositivo é sempre perigoso. Portanto, é o uso indevido dessa tecnologia que não é seguro, não o produto em si. Sempre depende de quem você permite conectar ao seu dispositivo e quais intenções essa pessoa realmente tem.

Imagine criar um perfil público nas mídias sociais e compartilhar todos os tipos de informações confidenciais publicamente. Não é a plataforma de mídia social que é insegura, é a forma como a plataforma está sendo usada naquele momento. O mesmo com um roteador de internet, por exemplo.

Imagine instalar um novo roteador em casa, mas desligar todos os firewalls. O dispositivo não é o problema, mas a maneira como essa tecnologia está sendo usada.

Manter-se vigilante e cauteloso no mundo online é importante. Isso também conta para a maneira como estamos usando tecnologias seguras. O descuido pode transformar as ferramentas mais seguras em portais abertos para os cibercriminosos se não prestarmos atenção.

Um exemplo

Estamos cientes que houve casos em que o AnyDesk e as ferramentas de outros provedores de Área de Trabalho Remota foram usados indevidamente em tentativas de phishing. Não toleramos o uso indevido de nosso produto e lutamos proativamente contra golpistas. Emparelhados com técnicas de engenharia social, os cibercriminosos podem alegar ser do seu banco ou provedor de internet, por exemplo. É provável que eles se aproximem de você por e-mail ou telefone, solicitando que você baixe uma Ferramenta de Área de Trabalho Remota, para poderem controlar ativamente seu dispositivo e ajudá-lo com um problema que, na realidade, não existe.

Os golpistas recentemente tentaram enganar as vítimas com um ataque de vishing, alegando estarem ligando da Amazon. Eles falsificaram números de telefone locais e explicaram que o objetivo da ligação era informar às vítimas que suas contas da Amazon haviam sido comprometidas. Os golpistas prometeram resolver o problema rapidamente se a vítima baixasse uma Ferramenta de Área de Trabalho Remota que concedesse acesso total ao computador. Na realidade, a conta da Amazon nunca havia sido invadida e a ligação era apenas um tru