● CUIDADO

Fiquem ligados no Pix!

Golpistas já criaram formas de roubar dados e prejudicar o consumidor na internet

A nova ferramenta para transferência instantânea e pagamentos, o Pix, só vai entrar em operação no dia 16, mas golpistas já criaram formas de prejudicar o consumidor. Ele roubam dados num canal de cadastro de chaves específicas nos bancos para fazer a transação. No quadro ao lado a Federação Brasileira de Bancos (Febraban) listou 25 medidas que ajudam o consumidor a manter seu ambiente virtual seguro.

E como funciona o golpe? Os cibercriminosos lançaram "iscas" pela internet solicitando o pré-cadastro para o sistema, inclusive por email. O objetivo seria coletar dados bancários e pessoais (como senhas de conta, celular e CPF), para que os golpistas possam ter acesso a uma futura conta Pix da vítima e efetuar transações em seu nome.

"O email que identificamos usava o nome de um banco popular e trazia um link para que o usuário fizesse o cadastro na conta Pix. O link em questão era direcionado a um site falso que simulava o banco e pedia que a vítima inserisse a sua senha bancária e seus dados", explica Fabio Assolini, analista sênior de cibersegurança da Kaspersky.

As chaves de segurança do Pix só devem ser registradas no aplicativo oficial do banco ou no site da entidade, nunca por meio de links recebidos por email, que são os pishings, ou WhatsApp.

"Os bancos e instituições financeiras não adotam esse procedimento. O correto é a pessoa entrar no site do banco, na página da instituição da qual é cliente, e preencher lá os dados para sua chave Pix. Os consumidores não devem acessar links recebidos por outros meios nem informar dados solicitados por telefone, por exemplo", alerta Rodrigo Alexandre, especialista da Proteste.

HOME OFFICE

- **Altere** credenciais de fábrica definidas pelo fabricante no wi-fi para uma conexão mais segura
- Faça as **atualizações** em seus equipamentos recomendadas pelo fabricante e use um antivírus
- **Evite** a utilização de soluções de serviços de VPN gratuitas e redes de wi-fi públicas

SENHA E AUTENTICAÇÃO

- **Troque** todas as suas senhas periodicamente (por exemplo: a cada 2 meses, ou sempre que houver suspeita de que sua senha foi comprometida)
- **Não compartilhe** senhas
- **Não utilize** a mesma senha para mais de um serviço
- **Não salve** senhas em cadernos, arquivos, no celular ou navegador
- Crie senhas **complexas**, com letras, números e caracteres especiais
- Use sempre a autenticação de **dois fatores** (ou verificação em duas etapas) que inclui uma segunda camada de autenticação para garantir o acesso
- Configure uma senha para acessar seu smartphone: **não use PIN ou padrão de desenho**. Se o seu dispositivo permite biometria ou reconhecimento facial, melhor ainda

PHISHING

- **Desconfie** de promoções imperdíveis. Mesmo que o remetente seja conhecido, ao abrir um anexo, **verifique** se há avisos sobre extensões que precisam ser ativadas
- **Oriente-se** para identificar um e-mail de phishing: o nome no endereço "De:" corresponde ao endereço de e-mail?, o texto está bem escrito ou contém erros ortográficos e gramaticais?, o logotipo está desfocado ou deformado?, está solicitando informações pessoais ou confidenciais?, há um senso de urgência na mensagem?, o endereço da página da internet é incomum? Se o tipo de arquivo parecer estranho, não abra
- **Cuidado** com mensagens de SMS (não clique em links, não forneça dados pessoais ou senhas)
- **Cuidado** com mensagens recebidas via WhatsApp ou Telegram (elas também podem ser maliciosas)
- **Não clique** em links desconhecidos
- Em tempos de pandemia, **tome cuidado** ao participar de **ações solidárias** transmitidas nas redes, mesmo que recebidas de pessoas conhecidas (existem sites e mensagens para captura de dados pessoais que induzem pessoas a compartilharem o phishing para ganharem produtos/serviços gratuitamente)

SEGURANÇA DO PIX

- Os cuidados que o cliente deverá adotar na hora de realizar uma transação através do Pix deverão ser os mesmos que adota ao fazer qualquer transação financeira. Portanto, **sempre confira** os dados do recebedor da transação Pix
- Os aplicativos móveis dos bancos devem ser instalados a partir das **lojas oficiais** da Apple (Apple Store) e do Google (Play Store)
- Cuidado com os e-mails ou mensagens de WhatsApp sobre convites de pré-cadastro do Pix. Na dúvida, **não passe** nenhuma informação
- **Cuidado** com ligações de "supostos funcionários" de bancos oferecendo o cadastramento do Pix ou mesmo oferecendo um serviço de atualização via conexão remota com o argumento de atualizar ou fazer um teste. Na dúvida, **desligue e entre em contato** com seu gerente
- **Não faça** transferência ou realize transações para supostamente fazer um teste na sua chave Pix. Isso não existe.

REDES SOCIAIS E PRIVACIDADE

- **Evite** expor informações pessoais, financeiras e corporativas nas redes sociais
- **Evite** expor exageradamente informações que possam passar a impressão de **ostentação**
- Configure a **privacidade** das suas postagens
- **Nunca coloque** suas informações pessoais em formulários de promoções sem verificar no site oficial da empresa a legitimidade da companhia