

11º Fórum PI

GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX



GT de Segurança I Motivadores, participantes e metodologia

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate

Ciclos de contribuições

Início das reuniões em dezembro de 2019

- ✓ 1º Ciclo – Apresentado no 07º Fórum PI – Fevereiro/20
- ✓ 2º Ciclo – Apresentado no 08º Fórum PI – Abril/20
- ✓ 3º Ciclo – Apresentação no 09º Fórum PI – Junho/20
- ✓ 4º Ciclo – Apresentação no 10º Fórum PI – Agosto/20
-  5º Ciclo – Apresentação no 11º Fórum PI – Outubro/20

Objetivos

Apresentar os aspectos de segurança mapeados que necessitam alguma revisão e novos riscos identificados, com seus respectivos planos de ação.

Participantes*

- | | |
|-------------|-----------------------|
| 1. ABBC | 11. ZETTA |
| 2. ABECS | 12. PSTI ABBC |
| 3. ABIPAG | 13. PSTI C&M SOFTWARE |
| 4. ABO20 | 14. PSTI JD |
| 5. ABRACAM | 15. SINDTELEBRASIL |
| 6. ABRANET | 16. TESOURO NACIONAL |
| 7. AGEV | 17. B3 |
| 8. AMPEF | 18. CIP |
| 9. FEBRABAN | 19. Claro |
| 10. PAGOS | 20. RTM |

* Participantes aprovados pelo Banco Central

GT de Segurança

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate

Agenda

- 1 > **Phishing – Links e APPs Falsos**
- 2 > **Campanhas de Conscientização Digital**
- 3 > **Análises Referentes ao Pix Copia e Cola**
- 4 > **Limites Transacionais**

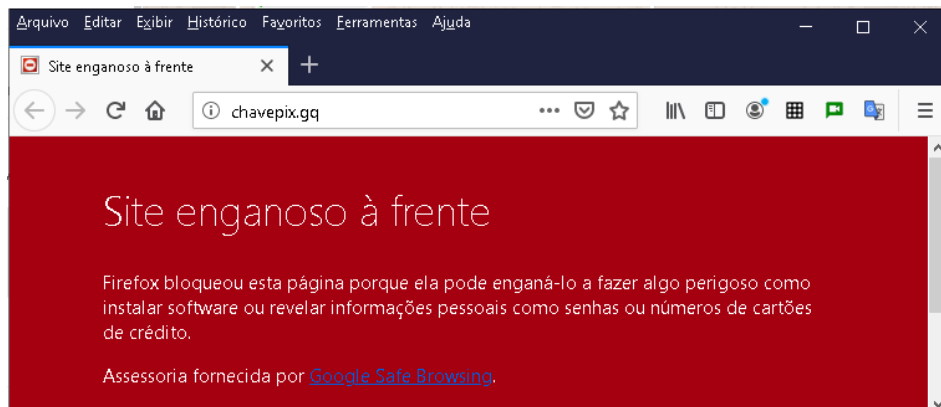
GT de Segurança I | 1 – Phishing – Links Falsos

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Cenário

Os serviços de monitoramento da marca e *takedown** identificaram que com a abertura do DICT para cadastro de chaves houve um aumento de domínios falsos registrados com a marca Pix.



```
ativarmeuaccess0.me
chavepix.me
chavepix.net
chavepix.online
clikpix.com.br
doarpix.com
doarpix.com.br
gerenciadorpix.com
pagarpix.com
pagarpix.com.br
pagarpix.net
pagopix.com
pagopix.com.br
pix-apkbb.tk
pix-aplicativos-clientes.tk
pixapp.online
pixbrasil.tech
pixempresa.com
pixempresas.com
pixpaga.com.br
primepix.com.br
santander.pixempresa.com
hb.pixempresa.com
bradesco.pixempresa.com
pixitajuridico.com
suportepix.online
vcfyg.ativarmeuaccess0.me
pix.atualizacaowebsegura.gq
pixcreditosimulacao.site/validate.php
pix.novoacesso.tk
cadastropixhb.com
pagamentoinstantaneopix.com.br
pixpayment.com
seupix.com
cadastropix.atualizacaodesktop.ml
```



Imagens veiculada nos grupos de segurança

*Ações de takedown visam remover conteúdo que, disponível na internet, viole direitos de terceiros.

GT de Segurança I 1 – Phishing – Links Falsos

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Cenário

Os serviços de monitoramento da marca e *takedown* identificaram que com a abertura do DICT para cadastro de chaves houve um aumento de domínios falsos registrados com a marca Pix.



Neste golpe o fraudador cria um link falso chamando atenção para o cadastro de chaves Pix.

Ao acessar o link, poderá ser requisitado ao cliente suas credenciais, que serão utilizadas depois para acessar os recursos do cliente.



Vários domínios são registros e apontam para “*Domain Parking*”, ou seja ficam inativos boa parte do tempo e são ativados por um curto período para aplicar golpes.

GT de Segurança I | 1 – Phishing – Links Falsos

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Experiência dos PSPs para *Takedown*



- Normalmente realizado de forma rápida (média 5 – 8 horas)
- Necessário efetuar ligações telefônicas
- Colaboração entre as instituições funciona com compartilhamento de informações
 - Contato dos principais provedores
 - Melhor forma de solicitar o *takedown*
- Reportado ao CERT BR e REGISTRO BR que realiza o bloqueio ou congelamento do domínio de forma rápida



- Processo moroso
- Muitas vezes só pode ser feito por formulário e não há um feedback
- Há pouca colaboração, pois poucos casos são atendidos. O Bloqueio ou congelamento quase nunca é efetivado
- Há evidências de URL ativa há mais de um ano

GT de Segurança I 1 – Phishing – Links Falsos

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Principais pontos de atenção

1. Provedores internacionais seguem legislação de cada país (existem leis fortes e fracas);
2. Vários domínios, inclusive os aparentes “*Domain Parking*” são ativados para fraude em um curto espaço de tempo (geralmente horas), somente enquanto o golpe é aplicado;
3. Algumas fraudes apontam para sites legítimos que foram invadidos para hospedar página falsa ou maliciosa. O *Takedown* nesses casos não é fácil, necessitando do dono do site realizar a operação;
4. Algumas instituições possuem o serviço de monitoramento da marca e *takedown*, mas por contrato isso não abrange fraudes/golpes onde o link não possui a marca monitorada.

Mitigadores

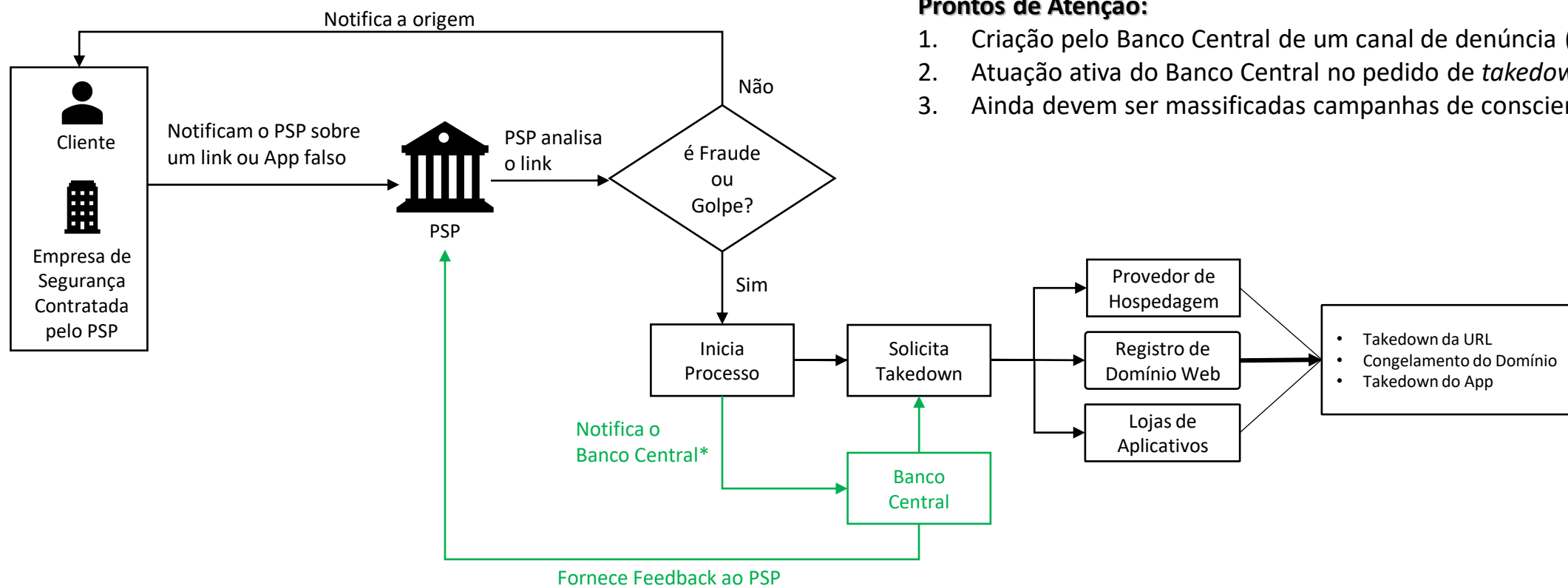
1. Criação pelo Banco Central de um canal de denúncia para links falsos do Pix;
2. Atuação ativa do Banco Central, como órgão regulador do setor Financeiro vinculado ao governo federal, solicitando o *takedown* com provedores nacionais e principalmente internacionais;
3. Campanhas de conscientização digital.

GT de Segurança I | 1 – Phishing – Links Falsos

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para a atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Fluxo Mitigador proposto



Prontos de Atenção:

1. Criação pelo Banco Central de um canal de denúncia (e-mail)
2. Atuação ativa do Banco Central no pedido de *takedown* aos provedores
3. Ainda devem ser massificadas campanhas de conscientização

GT de Segurança

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate

Agenda

- 1 > Phishing – Links e APPs Falsos
- 2 > **Campanhas de Conscientização Digital**
- 3 > Análises Referentes ao Pix Copia e Cola
- 4 > Limites Transacionais

GT de Segurança I 2 – Campanhas de Conscientização Digital

Contexto

Na Europa e USA existe o *Cyber Month*, um mês dedicado a campanhas de segurança digital. No Brasil esse movimento foi iniciado em 2019 com a Semana da Segurança Digital.

Semana da Segurança Digital – De 25 a 31 de Outubro

Criada em 2019 e alinhada com ações do *Cyber Month* que ocorre nos EUA (desde 2003) e Europa (2011), essa **iniciativa visa trazer Educação Digital para os brasileiros** em geral, de forma que estejam mais preparados para lidar com o mundo virtual.

Na primeira edição o foco foi em **conscientizar os clientes em como lidar com seus dados pessoais e financeiros**, dicas para não cair em golpes de ofertas tentadoras, boletos falso, *Phishing*, *SMSHING*, *Vishing*.

A campanha acontece na última semana de Outubro (mês das ações que acontecem fora do Brasil), auxiliando ações educativas para compras da Black Friday e também final de ano.

Não há necessidade de adesão, apenas o alinhamento dos tópicos tratados e uso das mesmas *hashtags* para melhor distribuição e monitoramento.

Neste ano os temas tratados serão:	Hashtags para a Semana de Segurança Digital
• Home office • Senha e autenticação • Phishing • Redes sociais e privacidade • <u>Segurança do Pix</u>	#SegurançaDigital [hashtag principal] #SemanadaSegurançaDigital #CompartilheSegurançaDigital

GT de Segurança I 2 – Campanhas de Conscientização Digital

Contexto

Na Europa e USA existe o *Cyber Month*, um mês dedicado a campanhas de segurança digital. No Brasil esse movimento foi iniciado em 2019 com a Semana da Segurança Digital.

Semana da Segurança Digital – Segurança no 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 (pagamento ou transferência), seja para uma pessoa ou um estabelecimento.



- **Não acesse links** encaminhados por **e-mails, postagens em mídias sociais** ou **SMS** provenientes de pessoas e órgãos duvidosos. **Sempre desconfie dos links que você recebe;**
- Faça o seu cadastro de sua **chave Pix** no ambiente seguro da sua instituição através do **Internet Banking ou Mobile Banking.**
- Os aplicativos móveis 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 cadastro do Pix. Na dúvida, **não passe nenhuma informação;**
- Cuidado com ligações de “**supostos funcionários**” de instituições 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.**

GT de Segurança

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate

Agenda

- 1 > Phishing – Links e APPs Falsos
- 2 > Campanhas de Conscientização Digital
- 3 > **Análises Referentes ao Pix Copia e Cola**
- 4 > Limites Transacionais

GT de Segurança I 3 – Análises Referentes ao Pix Copia e Cola

Contexto

A experiência de iniciação de um Pix em transações iniciadas e finalizadas em canal mobile, como transações realizadas no e-commerce e cobranças efetuadas por meio de aplicativos de mensagens, se dará através do Copia e Cola da *string* que representa o QR Code, estático ou dinâmico, gerado para iniciação de um Pix.

Pix Copia e Cola



Riscos

O Pix copia e cola apresenta um risco no que diz respeito a ataques de aplicações maliciosas no dispositivo do cliente.

Assim como ocorria no caso dos tradicionais “vírus de boleto”, onde um malware monitorava a área de transferência do dispositivo e ao detectar a presença de uma linha digitável alterava essa informação para corresponder a um boleto fraudulento, o mesmo poderia ser aplicado no Pix cópia e cola, onde o malware poderia trocar a informação copiada para forçar um pagamento indevido.

Mitigadores

- O PSP deverá apresentar ao usuário final pagador a informação do usuário final recebedor para confirmação da transação
- O processo de relato de infração poderá rapidamente detectar chaves usadas para golpes
- Os PSPs possuem processos internos de análise de transações suspeitas.
- Campanhas de conscientização digital

GT de Segurança

Contexto

O GT SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate

Agenda

- 1 > Phishing – Links e APPs Falsos
- 2 > Campanhas de Conscientização Digital
- 3 > Análises Referentes ao Pix Copia e Cola
- 4 > **Limites Transacionais**

GT de Segurança I 4 – Limites Transacionais

Contexto

Através da Instrução Normativa nº 20 o Banco Central divulgou os limites transacionais mínimos para o Pix em dois momentos, trazendo maior segurança para o início do ecossistema.

Limites Transacionais

Ademais dos pontos já tratados na Instrução Normativa nº 20 o GT SEG entende que:

»» Pix Agendado

Os PSPs devem seguir os mesmos limites estabelecidos pela IN 20º do Banco Central, facilitando a comunicação ao cliente final e mantendo os mecanismos de segurança propostos.

O limite a ser consumido pelo Pix agendado deve ser o limite do dia do pagamento, ou seja, o limite do D+ X.

»» Parâmetros Adicionais

Devido a particularidades de cada instituição na relação com o cliente e políticas individuais de risco os parâmetros:

- Recebedor usual
- Chave previamente cadastrada

Deverão ser definidos pelo próprio PSP. Caso haja alguma definição que implique em fraudes ao ecossistema o Banco Central poderá notificar o PSP.

GT de Segurança | 4 – Limites Transacionais

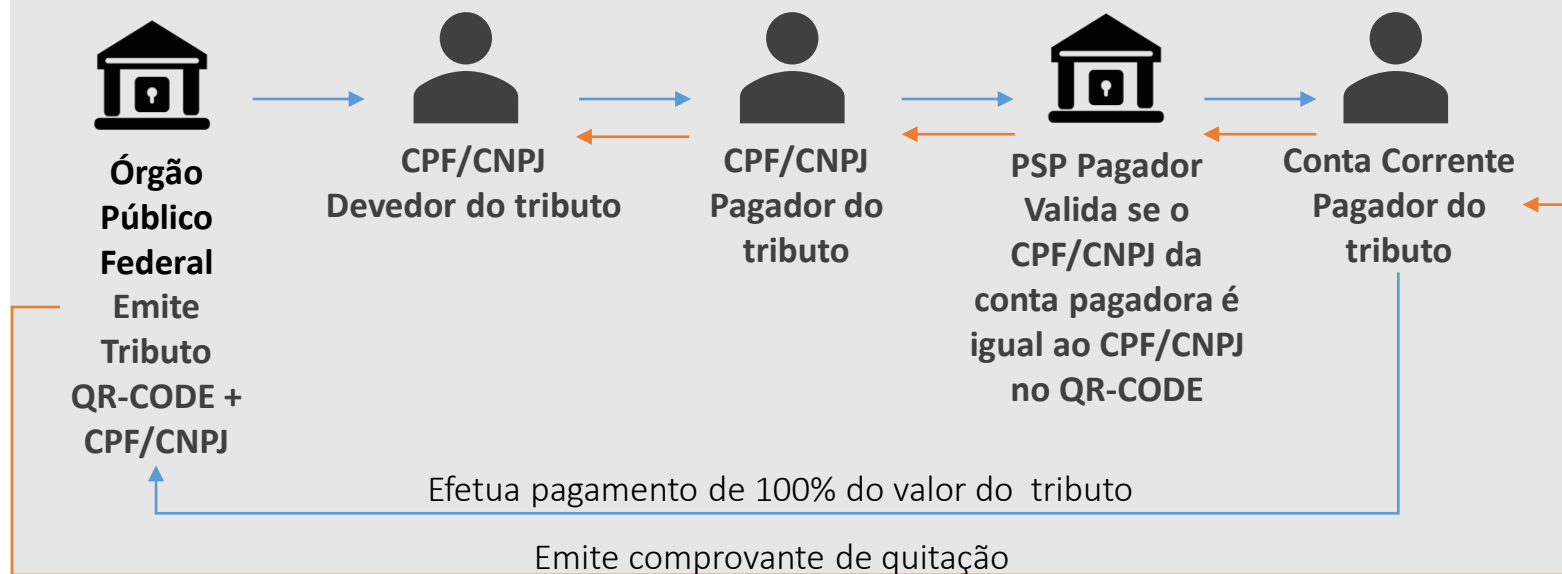
Contexto

Tratativa diferenciada para os pagamentos ao Tesouro Nacional.

Pontos de Atenção

- A grande maioria dos valores arrecadados por GRU são inferiores a R\$ 5.000,00
- Caso seja recebido do sistema do Órgão Público, o Tesouro enviará o CPF/CNPJ do Contribuinte Devedor. O Tesouro obrigatoriamente solicitará do Contribuinte Devedor o CPF/CNPJ para Valores maiores ou iguais a R\$50.000,00.
- A geração do QR-CODE dinâmico pelo Tesouro Nacional com os dados do CPF/CNPJ do Contribuinte Devedor será uma variável adicional de segmentação para os PSP's pagadores utilizarem no momento dos pagamentos, porém não será determinante.

Fluxo de Pagamentos do Tesouro Nacional



- Cada PSP Pagador deverá incorporar em sua estratégia de prevenção a fraudes a validação dos dados preenchidos no QR-CODE. (CPF/CNPJ + TIPO DO TRIBUTOS + VALOR DO TRIBUTOS)
- As estratégias podem variar em confirmação com o cliente, temporização ou até negar um pagamento de alto risco e/ou fraude confirmada.

IMPORTANTE no fluxo do Pix teremos o relato de infração e solicitamos ao Tesouro Nacional que seja avaliada uma forma de Alerta aos Órgãos Públicos Arrecadadores sobre o indício de fraudes.

11º Fórum PI

GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX

