Conscientização em Segurança da Informação para Clientes

Banco BNP Paribas

1. INTRODUÇÃO

De acordo com as políticas do **Banco BNP Paribas** sobre segurança na Internet, o portal BNP Paribas e suas áreas de negócio - **BNP Paribas Corporate & Institucional Banking (incluindo BP2S), BNP Paribas Asset Management** e **BNP Paribas Wealth Management** - mantém os mais altos padrões de segurança para evitar ações fraudulentas e a exposição de dados confidenciais.

Apesar destas medidas, o risco relacionado às operações *online* **não pode** ser completamente eliminado. Este documento propõe uma série de recomendações para aumentar a conscientização do cliente e a proteção de suas atividades *online*. Recomenda-se que esta página seja revista periodicamente para manter ciência das ameaças cibernéticas e das práticas de segurança adotadas do Banco.

2. RISCOS EM OPERAÇÕES BANCÁRIAS NA INTERNET

2.1. Malware

Malware, abreviação para *malicious software*, é um software usado ou programado por atacantes para interromper a operação do computador, coletar informações confidenciais ou obter acesso a sistemas de informação. *Malware* é um termo geral usado para se referir a uma variedade de formas de software hostil ou intrusivo, incluindo vírus de computador, *worms*, cavalos de Tróia, *key loggers*, *spyware* e outros programas maliciosos.

Os fraudadores costumam usar técnicas de *Phishing* ou Engenharia Social para instalar *malwares* em seu computador.

2.2. Engenharia Social

A engenharia social é um termo que descreve um tipo de intrusão que depende fortemente da interação humana, que tem como objetivo convencer e enganar outras pessoas para burlar controles de segurança.

O fraudador tenta - ao se apresentar como uma contraparte confiável - juntar informações suficientes para infiltrar a infraestrutura de uma organização.

Informação importante: o BNP Paribas **NUNCA** solicitará as suas credenciais de acesso à sua conta.

2.3. Phishing

O *phishing* é uma técnica fraudulenta de obtenção de informações privadas. Normalmente, o fraudador envia um e-mail que parece ser legítimo solicitando "verificação" de informações, seguido de um aviso sobre alguma consequência grave caso as informações não sejam fornecidas. O e-mail geralmente contém um *link* para uma página web - fraudulenta e idêntica a original, com logos e conteúdo da empresa – solicitando dados pessoais, que são usados para cometer roubo de identidade e / ou ações fraudulentas.

Informação importante: Recomenda-se que os clientes tenham cuidado e assegurem que os sites enviados por e-mails sejam legítimos antes de fornecer informações confidenciais. Os fraudadores muitas vezes atraem os clientes para usar suas credenciais (por exemplo: identificação de *login*, senha e números gerados a partir de dispositivos de segurança – ou *Tokens*) em páginas web falsas. Em caso de dúvidas, se possível, entre em contato com o remetente do e-mail e confirme se ele realmente enviou a mensagem.

3. PRÁTICAS DE SEGURANÇA DO BNP PARIBAS

O **BNP Paribas** está empenhado em proteger seus recursos de informações corporativas, dados em geral e informações do cliente. Esta declaração resume a abordagem da empresa para a segurança da informação. Ela fornece uma visão geral das medidas tomadas pela empresa para manter seguro a informação do cliente e garantir a confidencialidade, integridade e disponibilidade de dados. As características dessas medidas podem variar dependendo dos serviços prestados.

O **BNP Paribas** se esforça para lidar com dados de forma segura através de uma abordagem de defesa em profundidade (*defense-in-depth*), com o objetivo de proteger os ativos de informações do banco e de seus clientes contra a coleta, retenção, uso, divulgação, modificação ou destruição não autorizada. Isso é abordado através de políticas, procedimentos, diretrizes, arquitetura de segurança e da adoção de controles técnicos apropriados. A política e os controles de segurança da informação do banco são avaliados continuamente para garantir a relevância e o alinhamento com os padrões / requisitos de mercado. As políticas e os procedimentos da empresa fornecem cobertura de áreas críticas de segurança da informação, incluindo:

3.1. Controle de acesso

O acesso é concedido com um mínimo de privilégio e necessidade de saber. Todo o acesso é concedido com base em perfis de usuários e com aprovação prévia adequada na plataforma de Gerenciamento de Acessos. O uso de mídia removível é controlado e proibido por padrão.

3.2. Segurança de aplicações

Antes da implantação, as aplicações estão sujeitas a um processo de certificação de segurança para confirmar que foram desenvolvidas de acordo com nossa política de segurança de informações e padrões seguros de desenvolvimento de aplicativos. Auditorias regulares e testes de intrusão validam a força de aplicações sensíveis.

3.3. Controle de Mudança

As implantações de mudanças são controladas pelo uso de procedimentos formais de controle de mudanças. As mudanças exigem aprovação da área de Gerenciamento de Mudanças da implantação em ambiente de produção.

3.4. Disponibilidade de dados

As cópias de segurança de sistemas e dados são guardadas de forma segura para restauração em caso de necessidade. Sistemas de recuperação de desastres estão implantados para garantir a resiliência dos sistemas e dados em caso de indisponibilidade imprevista do ambiente de produção.

3.5. Confidencialidade de dados

Os protocolos seguros de rede são usados para tráfego sensível e complementados com soluções técnicas para detectar ou bloquear a extração de dados. A criptografia é empregada para transmissões de dados em redes públicas e em dispositivos de mídia portáteis.

3.6. Recuperação de desastres

O banco procura proteger pessoas, instalações, infraestrutura, processos de negócios, aplicativos e dados durante e após eventos catastróficos. A resposta e a recuperação de sistemas de aplicativos e processos de negócios críticos foram cuidadosamente planejadas e testadas. A metodologia de recuperação de desastres da empresa incorpora os seguintes itens:

- Análise de impacto de negócios.
- Planos de recuperação de desastres de missão crítica.
- Testes regulares de planos de recuperação de desastres para verificar a prontidão operacional.

3.7. Governança

As equipes de segurança ao redor do mundo são dedicadas a cooperar regional e globalmente no Grupo BNP Paribas. As equipes são estruturadas em polos especializados, garantindo uma cobertura permanente de aplicativos, sistemas e segurança de dados, bem como resposta apropriada aos incidentes de segurança. Um Gerente de Segurança da Informação (CISO) local supervisiona e mantém a estrutura de políticas de segurança e procura garantir que a estratégia de segurança seja apropriada para cobrir os riscos de segurança de maneira apropriados no que tange questões operacionais e regulatórias.

3.8. Recursos Humanos

Um programa de conscientização de segurança garante que os funcionários conheçam os riscos e possam agir adequadamente. As políticas de segurança garantem os deveres e responsabilidades dos funcionários em relação à proteção de dados.

3.9. Resposta a incidentes

Uma equipe regional de resposta a incidentes gerencia, controla e remedia incidentes relacionados à segurança da informação e monitora a eficácia dos controles. Os consoles de segurança do Banco são enriquecidos através de uma inteligência de ameaças controlada e externamente relevante para o cenário da ameaça.

Em caso de violação, a equipe de resposta a incidente prontamente tomará medidas para manter as informações seguras e mitigar a violação. As notificações oportunas de clientes afetados são emitidas de acordo com os requisitos contratuais, regulamentares e legislativos.

3.10. Defesa de rede

Os controles de acesso à rede estão em vigor para segregar segmentos de rede e filtrar o tráfego de entrada e saída com partes externas, além de monitoramento 24/7 e detecção de intrusão.

3.11. Segurança física

Medidas de segurança física estão instaladas e projetadas para fornecer acesso restrito e gravado, além de ajudar a detectar e dissuadir intrusões. Existem medidas para notificar o pessoal de segurança física de condições ambientais adversas que possam afetar os sistemas de comunicação eletrônica.

3.12. Defesa do sistema

Proteções contra *malwares* estão instaladas em todos os pontos-chaves da rede e são atualizadas regularmente para garantir a pronta detecção e eliminação de códigos maliciosos. Além disso, a aplicação de *baselines* de configuração de segurança garante a implantação de sistemas seguros. Um processo de correção garante que os sistemas estejam atualizados, com foco em atualizações de segurança. Análises de vulnerabilidades regulares asseguram que nenhum sistema tenha sido negligenciado.

3.13. Inteligência de ameaças

O **BNP Paribas** estabeleceu processos para a coleta e análise de ameaças no ciberespaço, especificamente adaptado aos cenários de ameaças recentes do banco e também do mercado, de maneira vertical. Esta função permanece à frente através de inteligência oportuna, precisa e relevante.

3.14. Gerenciamento de Fornecedores

O processo de Gerenciamento de Fornecedores do banco conduz diligências (*due diligences)* em atividades relacionadas à segurança da informação de terceiros e na aquisição, contratos e privacidade de dados, incluindo:

- Avaliação de potenciais fornecedores para o cumprimento das políticas e controles da empresa;
- Revisões de devida diligência, incluindo a elaboração de classificações de risco e resultados;
- Mitigação de resultados de risco;
- Suporte na seleção de fornecedores e negociações de contratos.

3.15. Gerenciamento de Vulnerabilidade

O time responsável pelo gerenciamento de vulnerabilidades verifica e analisa ativos de informações. Os controles mitigatórios e as correções serão aplicados, com priorização de ativos críticos.

4. RECOMENDAÇÕES AOS CLIENTES

Para evitar ações fraudulentas e exposição de dados confidenciais, o **BNP Paribas** recomenda aos seus clientes que levem em consideração uma série de diretrizes relacionadas ao gerenciamento do fluxo de trabalho e a proteção da infraestrutura resumida em 10 recomendações.

4.1. RECOMENDAÇÃO 1 – Implantar o princípio dos "*Quatro Olhos*"

O princípio dos "***Quatro Olhos***" indica que todas as operações realizadas devem ser analisadas por, no mínimo, duas pessoas. Respeite o princípio ***Quatro Olhos*** para todos os serviços principais, como gerenciamento de direitos, autorização de pagamento e gerenciamento de beneficiários.

4.2. RECOMENDAÇÃO 2 - Revisar o acesso do usuário

O responsável pelo controle de acesso deve revisar os acessos dos usuários pelo menos uma vez por ano.

4.3. RECOMENDAÇÃO 3 - Use versões de software atualizadas

Softwares incluem sistemas operacionais (exemplo: Microsoft Windows, Linux), navegadores (ex.: Internet Explorer, Firefox, Chrome) e outros softwares críticos (por exemplo: Java, Flash, Antivírus, *Firewall* e *Anti-Spyware*). Mantenha-os atualizados.

4.4. RECOMENDAÇÃO 4 – Manter o sigilo das informações pessoais

Senhas e *tokens* são informações pessoais e nunca podem ser compartilhadas com ninguém. É de extrema importância que as credenciais de *login* sejam garantidas, pois constituem os pontos de entrada das plataformas do BNP Paribas. As seguintes diretrizes podem ajudar a manter suas informações privadas seguras:

- Evite reutilizar os mesmos nomes de usuário e senhas que você usa para *logins* de outros sites;
- Não use informações que possam ser facilmente deduzidas;
- Mesmo que seu ID de usuário (geralmente o endereço de e-mail) não seja confidencial, não o anote em qualquer lugar que possa ser facilmente encontrada por uma pessoa mal-intencionada;
- Nunca anote ou revele sua senha para qualquer um que a solicite, incluindo as equipes de suporte do BNP Paribas. Certifique-se de que ninguém a conheça;
- Altere sua senha periodicamente;
- Certifique-se de que você não está sendo observado ao inserir sua senha;
- Verifique periodicamente o seu teclado e computador para garantir que nenhum *key logger* (dispositivos que gravam informações digitadas) esteja conectado;
- Muitos navegadores contêm funcionalidades de preenchimento automático. Enquanto isso economiza tempo para o usuário, ele também permite que pessoas não autorizadas façam *login* em sua conta se seu computador permanecer desbloqueado e sem alguém por perto. O banco recomenda que esta funcionalidade seja **desabilitada**.

Dispositivos de autenticação (quando aplicável):

- Certifique-se que *tokens* de autenticação ou senhas únicas enviadas para o dispositivo móvel, sejam mantidos em segurança o tempo todo;
- Não envie por e-mail e nem fale por telefone o número de série atrás de *tokens* de autenticação, mesmo que informem ser da equipe de suporte. A única exceção a esta regra é se você tenha entrado em contato com o Suporte Técnico para solicitar suporte.
- Nunca cole ou escreva informações no token de autenticação;
- Por último, mas não menos importante, se você perdeu ou acreditar ter perdido seu *token*, entre em contato com o seu gerente de Relacionamento do BNP Paribas para que possamos desativar o dispositivo o mais rápido possível.

4.5. RECOMENDAÇÃO 5 - Proteja sua estação de trabalho contra *malwares*

Proteja seu computador contra ***malwares***, vírus e programas maliciosos. Software antivírus, software *anti-spywar*e e *firewalls* pessoais devem ser instalados e continuamente mantidos ativos em seu computador. Os *patches* e correções de segurança e definições de vírus devem ser periodicamente instalados e atualizados para garantir que todos os erros e falhas de segurança sejam corrigidos. Execute periodicamente o software antivírus e *anti-spybot* com o intuito de detectar um arquivo suspeito. Caso detecte, exclua imediatamente o arquivo e feche o site que fez o download do arquivo. Se o computador for comprometido, não hesite em alterar todas as suas senhas. Não realize nenhuma transação através de computadores públicos ou compartilhados.

4.6. RECOMENDAÇÃO 6 - Não deixe sua estação de trabalho sem vigilância

Nunca se ausente de seu computador sem bloqueá-lo. Sempre encerre as aplicações após concluir transações bancárias eletrônicas.

É altamente recomendável fechar as telas dos navegadores após usar qualquer sistema do BNP Paribas.

4.7. RECOMENDAÇÃO 7 - Visite somente sites confiáveis

Visite apenas sites confiáveis e não faça download de nenhum arquivo ou programa de sites desconhecidos ou suspeitos. Tenha sempre cuidado ao abrir um arquivo desconhecido ou ao clicar em links suspeitos.

4.8. RECOMENDAÇÃO 8 – Tenha cuidado com mensagens de e-mail fraudulentas e também com os sites que afirmam ser do BNP PARIBAS

Mantenha-se vigilante ao receber e-mails suspeitos e ao acessar sites que afirmam ser do BNP Paribas com o intuito de obter informações confidenciais. O BNP Paribas nunca pedirá informações pessoais por e-mail e não enviará e-mails com links para que sejam acessados. Verifique sempre se o remetente de e-mail é conhecido e confiável antes de abrir qualquer anexo, e não responda ou clique em qualquer link fornecido nas mensagens de e-mail que parecem ser enviadas pelo BNP Paribas, solicitando que você insira dados pessoais, números de cartão / cartão bancário ou Códigos bancários de Internet.

Além disso, lembre-se de que, em alguns aplicativos de e-mail, como o *Microsoft Outlook*, um hiperlink de texto pode ser exibido, mas, na verdade, clicar no link pode direcioná-lo à outro site. Isso é conhecido como ***phishing***. Os sites de *phishing* são projetados para parecer idênticos aos sites reais. Além disso, alguns e-mails podem conter arquivos de imagem que aparecem como texto. Clicar na imagem também pode direcioná-lo a um site de *phishing*. Certifique-se de que as diretrizes para verificar os sites do BNP Paribas sejam seguidas.

Acessar o site do BNP Paribas deve sempre ser feito através de links conhecidos. Leia atentamente a barra de endereços / URL e sempre se certifique de que o domínio seja o esperado. Outro método para verificar a autenticidade do site BNP Paribas é verificar o certificado digital para sites que começam com "**HTTPS**". As Autoridades Certificadoras (como a Verisign ou a Geotrust) são emissores de terceiros de certificados digitais confiáveis que atestam se o site é genuíno. Clique no cadeado ao lado do URL para ver detalhes da Autoridade Certificadora.

4.9. RECOMENDAÇÃO 9 - Não atue em chamadas suspeitas do BNP PARIBAS

Se alguém entrar em contato com você alegando trabalhar para BNP Paribas ou atuando em nome do banco, solicitando que você forneça dados pessoais, ou que autorize transações, não execute ação alguma e entre em contato com o BNP Paribas através dos canais de contato adequados (**ver RECOMENDAÇÃO 10**).

4.10. RECOMENDAÇÃO 10 - Em caso de dúvidas entre em contato com o BNP PARIBAS

Encerrar imediatamente qualquer transação e entrar em contato com o BNP Paribas em caso de dúvida, especialmente quando o procedimento de assinatura difere do procedimento usual. É aconselhável verificar se as transações em curso são ou não legítimas. Entre em contato com o ponto de suporte nível um em caso de dúvida.

Em caso de suspeitas de acesso não autorizado ou em caso de dúvidas sobre questões relacionadas à Segurança da Informação, entre em contato imediatamente com seu Gerente de Relacionamento ou entre em contato através do e-mail Latam.CSIRT@bnpparibas.com.

5. AVISO LEGAL

Este documento foi elaborado pelo **BNP Paribas** apenas para fins informativos. Embora a informação contida neste documento tenha sido obtida de fontes que o **BNP Paribas** acredita serem confiáveis, não constituirá qualquer representação, garantia ou incentivo do banco quanto à adequação, exatidão ou suficiência das medidas aqui descritas para quaisquer propósitos contemplados, pois as informações podem estar incompletas ou resumidas.

Este documento não constitui um prospecto ou solicitação. Todas as estimativas e opiniões incluídas neste documento constituem o nosso julgamento a partir da data do documento e podem estar sujeitas a alterações sem aviso prévio. Mudanças nas premissas podem ter um impacto relevante em qualquer recomendação aqui feita.

Este documento não pode ser reproduzido (no todo ou em parte) para qualquer outra pessoa sem a prévia autorização por escrito do **BNP Paribas.**