Quatro dicas para se proteger contra golpes do Pix

A alta adesão ao Pix que, segundo o Banco Central, já tem mais de 253 milhões de chaves cadastradas e supera 2 bilhões de transações, tem atraído a sanha dos contraventores

No tópico golpes do pix a Serasa explica como a recente modalidade digital de transferência bancária gratuita, ágil, acessível e popular se tornou um meio para tentativas de fraudes.

Especialistas da Serasa orientam os usuários a identificar as fraudes mais frequentes e explicam os principais mecanismos utilizados pelos criminosos para atrair suas vítimas. Quatro dicas sobre os principais golpes do Pix e como evitá-los

Marcello Casal Jr/ABr

O Pix, transferência bancária gratuita, ágil, acessível e popular se tornou um meio para tentativas de fraudes.

1) **WhatsApp clonado -** O estelionatário se passa por uma empresa e pede que o usuário digite um código. O objetivo é clonar o número e pedir dinheiro para parentes e amigos da vítima. **Como evitar:** habilite a autenticação de duas etapas na sua conta do WhatsApp para que o criminoso não consiga mudar o cadastro, e não forneça nenhum código solicitado.
2) **Atendente bancário falso -** O golpista se passa por atendente do banco e induz a vítima a criar uma chave Pix e a transferir dinheiro para outra conta. **Como evitar:** nunca forneça seus dados ou faça operações bancárias por meio de ligações telefônicas.
3) **Bug do Pix -** Fake news nas redes sociais anunciam uma "falha" no Pix, pela qual as pessoas receberiam prêmio em dinheiro quando transferissem valores para determinadas chaves. É claro que o dinheiro vai direto para a conta do criminoso. **Como evitar:** fique alerta para notícias de dinheiro fácil, confirme a veracidade da informação e do perfil procurando por selos de verificação nas redes sociais oficiais, saiba que o sistema Pix, criado pelo Banco Central, é seguro, sem bugs e tem os mesmos protocolos de segurança do TED e do DOC.
4) **QR Code falso -** golpistas falsificam QR Code para transferências por Pix em lives e apresentações online que arrecadam dinheiro para artistas ou instituições. **Como evitar:** ao fazer doações, transferências e pagamentos por Pix utilizando QR Code fique atento à origem do código e, se desconfiar dos valores ou da solicitação, não faça a operação.

Outras dicas para não cair em golpes com o Pix:

- Antes de transferir qualquer valor verifique a identidade de quem está solicitando o Pix.
- Preste bastante atenção antes de clicar para confirmar uma operação e confira todos os dados.
- Não clique em links recebidos por e-mail, mensagens de SMS, WhatsApp e redes sociais que direcionam a cadastros de chaves Pix.
- Cadastre suas chaves Pix no canal oficial do seu banco ou fintech e saiba que a confirmação da criação da chave Pix nunca vem por ligação ou link. Após o cadastro, o Banco Central envia o código apenas por SMS ou e-mail
- Não faça transferências para pessoas conhecidas sem antes confirmar por chamada telefônica ou pessoalmente. - Fonte e outras informações: (https://www.serasa.com.br/premium/).

Os principais problemas de obras e como evitá-los

Um profissional de arquitetura e construção civil já sabe que fazer a gestão de uma obra é uma tarefa complicada e que requer vários cuidados. Pensando nisso, a Taíse Arioli, Arquiteta e Líder de Comunidades e Parcerias na Vobi, separou algumas dicas que podem ajudar a evitar essas complicações.

1) **Planejamento de obras** - Antes de tudo, a organização dos processos é essencial. Por isso, o planejamento é uma etapa importante para evitar possíveis problemas. Tenha em mãos todas as informações de atividades e a ordem em que precisam ser executadas.
2) **Orçamento e prazos com fornecedores -** Depois que o projeto estiver finalizado, é possível fazer uma estimativa dos produtos da obra e das tarefas de profissionais terceirizados. Por isso, é tão importante deixar o orçamento completo, detalhando valores das etapas para trazer mais segurança ao cliente. Depois que todos os detalhes do orçamento estiverem concluídos, é fundamental checar e estar atento ao tempo estimado que cada fornecedor necessita para executar os serviços.
3) **Problemas no controle e gestão de tempo -** Uma das maiores dificuldades é a gestão de tempo, pois possíveis atrasos em processos de uma obra podem resultar em custos adicionais por um cálculo errado na quantidade de horas que uma etapa é realizada, além de outros problemas.
Exatamente por isso, o cronograma de obras é essencial para organizar até os mínimos detalhes. Hoje em dia, é possível realizar etapas como essa de forma prática, rápida e totalmente online, como é o caso da Vobi, plataforma que otimiza tempo na gestão de projetos e desenvolvimento de negócios para profissionais do setor de arquitetura e construção civil.
4) **Gestão de insumos e desperdício de materiais -** Após a compra dos materiais e itens necessários para a obra, pode acontecer um problema muito comum: o desperdício de produtos. Por isso, é fundamental ter bastante cuidado e atenção na utilização dos insumos, além da armazenagem correta de cada um.
5) **Chuvas e mudanças climáticas -** Para não ser pego de surpresa por mudanças climáticas que podem interferir completamente no cronograma de obras e causar diversos problemas, é de extrema importância estar atento à previsão do tempo na região.

Portanto, realize um estudo de clima no local da obra e esteja sempre acompanhando o dia a dia para que consiga preferir esses problemas. - Fonte e outras informações: (www.vobi.com.br).

Prepare seu SOC para os novos desafios cibernéticos

Marco Alexandre Garcia (*)

Quanto mais descentralizadas são as operações das empresas, maiores são os desafios para garantir integridade das redes corporativas, protegendo dados e aplicações

Dados do '2021 Ransomware Study', do IDC, apontam que cerca de 37% das companhias ao redor do mundo afirmam ter sofrido ataque por ransomware no ano passado. O FBI também traz dados alarmantes. Segundo a divisão cibernética do órgão norte-americano de defesa, o número de ataques reportados à área aumentou 400% com a pandemia da Covid 19.

Nesse cenário, muitas empresas entenderam que prevenir, identificar e mitigar riscos cibernéticos é resultado de um conjunto de ações que envolvem ferramentas e pessoas reunidas em centros operacionais dedicados à identificação de vulnerabilidades e resolução de incidentes nos sistemas de dados, conhecidos como Centro de Operações de Segurança, ou SOCs.

O SOC funciona como um "centro nervoso", 24x7 (24 horas do dia, sete dias por semana), onde eventos suspeitos são identificados e analisados com metodologias de detecção e proteção contra ameaças, tanto de modo manual, com base em procedimentos escritos, quanto de forma automatizada, por meio de ferramentas capazes de gerar alertas, notificações e até mesmo bloquear dispositivos ou acessos de usuário entre outras ações preventivas e corretivas.

Na mesma medida em que as tecnologias de proteção de dados se desenvolvem e os especialistas em cibersegurança correm para se antecipar às ações de hackers maliciosos, na tentativa de prevenir ataques, invasões, vazamento e sequestro de informações, a indústria do cibercrime se aperfeiçoa rapidamente, adotando novas estratégias que também envolvem tecnologia e pessoas, o que inclui a criação de abordagens da chamada engenharia social – truques psicológicos que levam o usuário a abrir portas de entrada em suas redes para agentes maldosos.

Para acompanhar esse contexto dinâmico, automatizar ao máximo as tratativas dos eventos de segurança (automated incident response), garante uma reação rápida e sem falhas às ameaças e agilidade para mitigar riscos cibernéticos. Com a automação de parte dos processos de detecção e mitigação de incidentes, os profissionais de cibersecurity – cada vez mais raros e disputados globalmente - ganham autonomia para dedicarem-se aos casos mais complexos.

Um caminho assertivo para a reforçar a automação nos SOCs das organizações é a adoção de ferramentas de SIEM (Security Information and Event Management), que otimizam a entrega de relatórios sobre atividades maliciosas, como comportamento anormal de usuários, tentativas suspeitas de login e outros, e emitem alertas acionados pelo mecanismo de análise se foram identificadas violações às regras de negócio, o que pode sinalizar um problema de segurança.

Outra forma de potencializar a cibersegurança é a adoção de Serviços de Detecção e Resposta Gerenciadas (ou MDR), que são apontados pelo IDC como tecnologias em ascensão, utilizando ferramentas avançadas de detecção, como EDR/XDR. Embora, em qualquer lugar do mundo, centros operacionais de segurança sigam um padrão similar de atuação, podemos dizer que a arquitetura customizada e aderente a cada modelo de negócio é a chave para uma proteção de dados mais eficiente.

No entanto, observamos diariamente gaps relacionados à conscientização e compliance dentro das organizações. Mesmo sendo claro para as empresas que a cibersegurança é um tema multidisciplinar associado ao comprometimento de toda a organização, ainda são comuns as limitações de engajamento e comunicação entre a área de SI (Sistemas da Informação) e demais áreas de suporte de TI, o que tem impacto considerável na eficiência do serviço.

Em outras palavras: não bastam ferramentas de proteção. Pessoas e processos ainda são fundamentais para que se atinja um nível aceitável de maturidade. Ao implementar ou atualizar um SOC, vale considerar uma estratégia de compliance e conscientização a partir do onboarding.

(*) - É Diretor de MSS LATAM da Cipher.

Hotel Majestic S/A

CNPJ 43.121.946/0001-19 - NIRE 35300033493

Assembleia Geral Extraordinária - Convocação

Prezado Senhor(a) Com fundamento no artigo 123, da Lei das S.A., a pedido dos acionistas Edgar José Bernardi, Olivia Faria Bernardi, HP Bernardi Participações Ltda e Ercy B. Bernardi Alencastro ficam os Senhores Acionistas do Hotel Majestic S/A. ("Companhia") convidados a se reunir em Assembleia Geral Extraordinária a ser realizada no dia 18 de agosto de 2022, às 11:00 hs no endereço da sede da Companhia, na Praça Dr. Vicente Rizzo, 160, nesta Cidade de Águas de Lindóia, Estado de São Paulo, para deliberar sobre a instituição do Conselho Fiscal e eleição de seus membros. Águas de Lindóia, 22 de julho de 2022. **José Artur Bernardi** - Diretor Presidente

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: https://www.portaldeassinaturas.com.br/Verificar/18E3-D29F-F605-6E98 ou vá até o site https://www.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 18E3-D29F-F605-6E98

Hash do Documento

65790F51AB9A6FB30F7E8178E2E4D6090B32F8B1E3A16BFE5EB82A8C2C439D21

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 25/07/2022 é(são) :

☑ Jornal Empresas & Negócios Ltda - 008.007.358-11 em 25/07/2022 20:09 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Autenticação de conta

Evidências

Client Timestamp Mon Jul 25 2022 20:09:19 GMT-0300 (Horário Padrão de Brasília)
Geolocation Latitude: -23.4937919 Longitude: -46.7234606 Accuracy: 18.026
IP 177.138.249.200
Hash Evidências:
35D2272037D19F3C53AA74CFC684CF72EECEDF459D4B61A6095B29E24A250C34

LEIA O QRCODE ABAIXO E ACESSE A PUBLICAÇÃO EM NOSSO PORTAL

https://jornalempresasenegocios.com.br/publicidade_legal/hotel-majestic-s-a-3/

Empresas & Negócios