Prefeitura de Jundiaí

Claudia George Musseli Cezar <ccezar@jundiai.sp.gov.br>

Segurança da Informação - Proteja-se contra Vishing

1 mensagem

'sac Serviço de Atendimento ao Cliente' via Segurança da Informação - CIJUN <segurancainformacao@jundiai.sp.gov.br>
Responder a: sac Serviço de Atendimento ao Cliente <sac@cijun.sp.gov.br>
Cco: segurancainformacao@jundiai.sp.gov.br

4 de fevereiro de 2025 às 09:30

Claudia George Musseli Cezar <ccezar@jundiai.sp.gov.br>

Alguns tipos de Golpe do Pix para ficarmos atentos em 2025

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br>
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Para: colaboradores@cijun.sp.gov.br
Cco: funcionarios-pmj@jundiai.sp.gov.br

9 de janeiro de 2025 às 08:08

CIJUN
Companhia de Informática de Jundiaí

Prezados(as),

Golpes no Pix: Como se Proteger em 2025

O **Pix** se tornou o meio de pagamento mais utilizado pelos brasileiros, mas sua popularidade também tem atraído golpistas que aplicam fraudes digitais. Por isso, é fundamental estar atento aos golpes mais comuns envolvendo o Pix, especialmente para reforçar sua segurança em 2025.

De acordo com uma pesquisa do Canaltech, o prejuízo médio causado pelos golpes do Pix é de **R$2.100**, um valor superior ao salário mínimo no Brasil, que é de **R$1.412**. Essas fraudes podem envolver desde vendas falsas de produtos e serviços até golpes de engenharia social, como a clonagem de números de WhatsApp.

A seguir, apresentamos alguns dos golpes mais recorrentes relacionados ao Pix, para que você possa se proteger e evitar prejuízos.

Fique atento para evitar cair em fraudes e proteger suas transações financeiras.

1. **Golpe do QR Code Falso**

Um golpe comum envolve a criação de QR Codes falsos para pagamentos via Pix. Nesse tipo de fraude, o golpista gera um código que direciona o pagamento para a sua própria chave, ficando com o dinheiro. Esse tipo de golpe pode ocorrer tanto em lojas online quanto em estabelecimentos físicos que utilizam códigos fixos.

Dicas de segurança:

- **Sempre prefira digitar a chave Pix manualmente.**
- **Compre em lojas que utilizam QR Codes temporários, que são mais seguros.**

Em lojas físicas:

- **Fique atento a QR Codes que parecem borrados, mal colocados ou que estão colados com fitas, adesivos, etc.**
- **Se tiver dúvidas, não faça o pagamento! Procure um responsável pela loja e verifique se o QR Code está correto.**

Em compras online:

- **Se desconfiar da origem do QR Code ou do link fornecido, entre em contato diretamente com a empresa antes de realizar o pagamento.**

Sempre confirme a autenticidade do QR Code antes de realizar qualquer pagamento. Na dúvida, não faça o Pix. A segurança da sua transação é fundamental!

2.Golpes no WhatsApp: Como se Proteger

O WhatsApp é frequentemente utilizado por criminosos para aplicar fraudes financeiras. Além do golpe do QR Code, golpistas podem clonar contas de amigos ou familiares da vítima, se passando por eles para solicitar dinheiro em situações de emergência. Também é comum que empresas sejam clonadas, com golpistas usando perfis falsos para vender serviços inexistentes.

Como se proteger:

- Preste atenção no número de telefone que está entrando em contato com você. Verifique se o número corresponde ao da pessoa ou empresa em questão.
- Se receber uma solicitação suspeita, entre em contato diretamente com a pessoa ou empresa por outro meio, para confirmar a veracidade do pedido.

Sempre desconfie de pedidos inesperados de dinheiro e, se possível, faça a verificação antes de realizar qualquer pagamento. Segurança em primeiro lugar!

3. Golpes de Compras e Sorteios Falsos

Descontos excessivos e promoções irresistíveis podem ser um sinal de alerta. Em alguns casos, essas ofertas podem ser armadilhas criadas por cibercriminosos. Golpistas podem criar sites falsos que imitam marcas conhecidas ou entrar em contato para informar que você "ganhou" um prêmio, mas para recebê-lo, será necessário pagar uma taxa.
No caso de lojas falsas, é comum que os sites ofereçam apenas o Pix como forma de pagamento, pois isso dificulta o reembolso caso você se arrependa. Para evitar cair nesse tipo de golpe, sempre verifique a identidade da empresa e, se possível, procure por opções de pagamento mais seguras, como cartão de crédito.

Dicas de segurança:

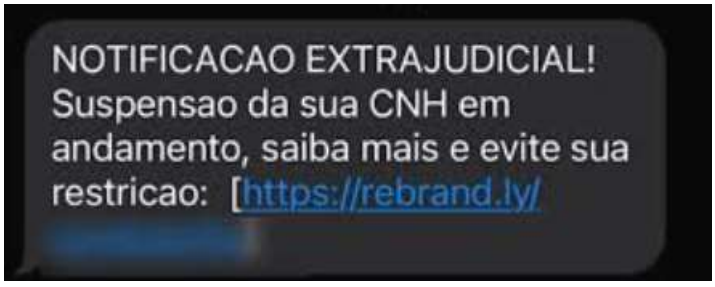
- Desconfie de ofertas com preços muito abaixo da média.
- Sempre confirme a autenticidade do site e da empresa antes de realizar qualquer compra.
- Prefira métodos de pagamento que oferecem mais proteção, como o cartão de crédito, que permite contestar cobranças.

Se tiver dúvidas, não finalize a compra sem antes fazer uma verificação. Segurança é a chave para evitar fraudes!

4. Golpes da CNH e da Entrega dos Correios

Esses golpes se tornaram populares em 2024 e é provável que novas versões surjam em 2025. Nesse tipo de fraude, o criminoso envia um SMS informando que é necessário pagar uma taxa para liberar uma encomenda supostamente retida nos Correios ou para regularizar a Carteira Nacional de Habilitação (CNH). A mensagem contém um link que leva a um site falso, que imita a identidade das instituições responsáveis, onde é solicitado um pagamento.

O pagamento geralmente deve ser feito via **Pix**, o que dificulta a devolução do dinheiro, pois ele é enviado para uma conta "laranja". Esse tipo de golpe, que leva a vítima a clicar em um link malicioso, é conhecido como **phishing**.



Como se proteger:

- **Desconfie de mensagens não solicitadas**, especialmente aquelas com links que pedem pagamento para liberar encomendas ou regularizar documentos.
- **Não clique em links** enviados por SMS. Em vez disso, entre em contato diretamente com os Correios ou o órgão responsável para verificar a veracidade da informação.
- Prefira usar formas de pagamento mais seguras, como cartão de crédito, que oferecem maior proteção.

Se você receber uma mensagem suspeita, **não faça o pagamento** e denuncie o golpe. A segurança online depende da nossa atenção e cautela!

5. Golpes por Aproximação

Em 2025, o **Pix por aproximação** deve se tornar amplamente disponível, com o lançamento geral previsto para fevereiro. Algumas empresas já estão testando essa ferramenta, que promete agilizar os pagamentos. No entanto, assim como qualquer inovação, ela também exige atenção para garantir a segurança das transações.

Além do **Pix por aproximação**, os golpistas podem explorar a tecnologia de pagamentos por aproximação de cartões de crédito e débito. Nesse tipo de golpe, criminosos podem usar dispositivos para fazer pagamentos sem o consentimento da vítima, aproximando suas maquininhas de forma furtiva. Outra fraude comum é o golpe da maquininha falsa, onde o golpista informa que o pagamento por aproximação não está funcionando e solicita que o cartão seja inserido em uma máquina que pode clonar o cartão ou registrar valores errados.

Como se proteger:

- **Sempre verifique o valor antes de autorizar qualquer pagamento**, especialmente se o pagamento for feito por aproximação.
- **Desconfie se a maquininha não estiver funcionando corretamente**. Se alguém pedir para você inserir o cartão fisicamente, esteja atento, pois pode ser uma tentativa de clonagem.
- **Use carteiras digitais ou senhas adicionais**, quando possível, para aumentar a segurança das suas transações por aproximação.

Com a adoção do Pix por aproximação, é importante manter-se vigilante e adotar boas práticas de segurança para evitar prejuízos.

6. Golpe da Falsa Central Bancária

Neste golpe, os criminosos entram em contato com a vítima por telefone ou mensagem, se passando por representantes de uma central de atendimento de um banco. Eles alegam que há uma suposta compra fraudulenta ou um problema urgente que precisa ser resolvido através da conta da vítima, com o objetivo de obter seus dados de acesso.

Por envolverem grandes quantias de dinheiro e alegações de assuntos urgentes, esse tipo de golpe tem causado muitos prejuízos. Vale destacar que os bancos **nunca** solicitam dados sensíveis durante ligações telefônicas.

Como se proteger:

- **Não forneça nenhuma informação pessoal**, como senhas, códigos de segurança ou dados bancários, por telefone.
- Se receber um contato suspeito, **desligue imediatamente** e entre em contato diretamente com o banco por meio do número oficial disponível no site da instituição.
- Em caso de dúvida, sempre busque formas seguras de verificar a situação, como acessar sua conta bancária diretamente pelo aplicativo ou site oficial.

Atenção redobrada e precaução são essenciais para evitar cair nesse golpe.

7. Golpe da Falsa Devolução

O **Mecanismo Especial de Devolução (MED)** foi criado pelo Banco Central do Brasil para ajudar a proteger vítimas de fraudes financeiras, permitindo a recuperação de valores transferidos por engano. No entanto, golpistas têm se aproveitado desse recurso para causar prejuízos às vítimas.

No **Golpe do Pix Errado**, a vítima recebe uma transferência indevida e, logo depois, é contatada pelo golpista solicitando a devolução do valor. Porém, o pagamento deve ser feito para uma **Chave Pix** diferente da original. O criminoso utiliza o

MED para tentar recuperar o dinheiro enviado.

Como se proteger:

- **Sempre confirme os dados** da Chave Pix antes de realizar qualquer devolução. Verifique se a chave e os dados do beneficiário correspondem corretamente.
- Se receber um pedido de devolução de um valor transferido, entre em contato diretamente com o remetente ou o banco para confirmar a legitimidade do pedido.

Ao desconfiar de qualquer solicitação, **não faça o pagamento** sem antes verificar a situação. Evite cair nesse golpe e proteja suas finanças.

8. Aplicativo de Pagamento Falso

Este golpe pode afetar principalmente comerciantes, sendo uma forma de fraude onde golpistas utilizam **aplicativos falsos** que simulam a interface de um banco. O criminoso gera um **comprovante falso de pagamento via Pix**, levando o comerciante a acreditar que a transação foi concluída. No entanto, o pagamento nunca é realizado, e o golpista sai com o produto sem pagar.

Como se proteger:

- **Sempre confirme se o pagamento foi realmente recebido** antes de liberar o produto ou serviço. Verifique o saldo da conta para garantir que o valor entrou corretamente.
- **Desconfie de comprovantes de pagamento** gerados por aplicativos desconhecidos ou que apresentem informações suspeitas.

Dicas de segurança:

- **Não se deixe levar por mensagens urgentes** ou pressões para realizar a venda rapidamente. Golpistas tentam criar um senso de urgência para que você não tenha tempo de verificar a transação.
- **Valide sempre as transações** e em caso de dúvida, entre em contato diretamente com o banco ou plataforma de pagamento.

A chave para evitar esse tipo de golpe é a **atenção e a cautela**. O desespero e a pressa são os maiores aliados dos criminosos.

Fontes : [8 golpes de Pix para ficar atento em 2025 - Canaltech]

pix - TheWebGuardian

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Cuidado com o crachá: Proteja suas informações e a segurança da empresa | órgão público

1 mensagem

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 21 de fevereiro de 2025 às 09:51
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Para: colaboradores@cijun.sp.gov.br
Cco: funcionarios-pmj@jundiai.sp.gov.br

CIJUN
Companhia de Informática de Jundiaí

Prezados(as),

Certamente você já deve ter visto alguma pessoa postando fotos com o crachá da empresa | órgão público em redes sociais, principalmente o Linkedin. Correto? A princípio, parece inofensivo mas, essa inocente ação pode colocar tanto a pessoa como a empresa | órgão público em risco. Às vezes, nós mesmos, na correria do dia a dia, ou mesmo distração, esquecemos e saímos pelas ruas com o crachá exposto, o colocamos na mesa do restaurante, etc. Pensando nestas situações, citamos abaixo algumas razões pelas quais estas ações são potencialmente perigosas :

1. **Informações Expostas**: O crachá geralmente contém dados como nome, cargo, , rg, cpf,setor e até o logo da empresa | órgão público. Essas informações podem ser usadas por pessoas mal-intencionadas para falsificar identidades, praticar golpes ou até para facilitar ataques cibernéticos à empresa.
2. **Facilidade para Engenharia Social**: Criminosos podem usar as informações do crachá para tentar enganar funcionários ou terceiros, se passando por colaboradores da empresa | órgão público em situações de golpe ou fraude, seja por e-mail, telefone ou pessoalmente.
3. **Acesso Físico Indesejado**: Se o crachá contiver dados sobre permissões de acesso, um golpista pode tentar replicá-lo ou até usar sua imagem para tentar invadir a sede da empresa | órgão público. Mesmo fora da internet, andar com o crachá exposto em público pode atrair olhares curiosos que podem capturar suas informações.
4. **Privacidade e Reputação**: Compartilhar fotos do crachá ou andar com ele à mostra também expõe sua privacidade e a imagem da empresa | órgão público, que pode não querer que informações internas ou de segurança estejam acessíveis ao público.

O Que Fazer?

- **Evite postar fotos com crachá**: Mesmo que pareça uma lembrança inocente de um evento ou do primeiro dia de trabalho, omita o crachá das fotos que você compartilha online.
- **Guarde Seu Crachá em Local Seguro**: Quando estiver fora do ambiente de trabalho, mantenha o crachá guardado e fora de vista.
- **Atenção ao Uso em Eventos Externos**: Em eventos e conferências, após entrar no local, guarde o crachá para evitar que ele seja visto por pessoas que não deveriam ter acesso a essas informações.

- **Revise Suas Configurações de Privacidade**: Caso tenha compartilhado fotos no passado, revise as configurações de privacidade de suas redes sociais e, se possível, remova imagens onde o crachá esteja visível. Lembre-se de que mesmo amigos ou seguidores podem compartilhar inadvertidamente essas informações.
- **Use Protetores de Crachá**: Sempre que possível, utilize protetores de crachá opacos ou com mecanismos de travamento que dificultem a visualização por terceiros. Assim, caso precise usá-lo ao transitar entre áreas, as informações sensíveis ficam protegidas.
- **Cuide da Etiqueta de Segurança no Trabalho**: Incentive seus colegas de trabalho a fazerem o mesmo. Cuidado com o uso de crachás, principalmente em áreas comuns, pode ser uma excelente prática coletiva que aumenta a segurança da empresa como um todo.
- **Reporte Suspeitas Imediatamente**: Caso note atividades suspeitas relacionadas ao uso ou exposição de crachás na sua empresa | órgão público, informe imediatamente o setor de segurança para que medidas preventivas possam ser tomadas.

Lembre-se: pequenos cuidados com o seu crachá ajudam a proteger não só você, mas também a segurança e a reputação da sua empresa | órgão público.

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Segurança da Informação - Use redes wi-fi seguras

1 mensagem

'sac Serviço de Atendimento ao Cliente' via Segurança da Informação - CIJUN 18 de fevereiro de 2025
<segurancainformacao@jundiai.sp.gov.br> às 09:30
Responder a: sac Serviço de Atendimento ao Cliente <sac@cijun.sp.gov.br>
Cco: segurancainformacao@jundiai.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Treinamento SEI - Melhores Práticas

1 mensagem

'sac Serviço de Atendimento ao Cliente' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 24 de fevereiro de 2025 às 13:12
Responder a: sac Serviço de Atendimento ao Cliente <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br
Cc: Funcionários Cijun <funcionarioscijun@cijun.sp.gov.br>

Passando para lembrar que **hoje dia 24/02/2025 às 14 horas**, teremos nosso primeiro treinamento do SEI de Melhores Práticas.

O treinamento terá duração de aproximadamente 1 hora e será uma excelente oportunidade para aprimorar o uso do sistema.

Não é necessário inscrição prévia, basta acessar o link.

24/02 (segunda-feira) às 14 horas - Melhores Práticas

link de acesso: meet.google.com/zqs-uxea-syt

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Cuidado com prints e fotos de tela!

1 mensagem

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 28 de fevereiro de 2025 às 09:34
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Para: colaboradores@cijun.sp.gov.br
Cco: funcionarios-pmj@jundiai.sp.gov.br

CIJUN
Companhia de Informática de Jundiaí

Cuidado com prints e fotos de tela

Prezados(as),

Este comunicado é um alerta sobre um comportamento que, num primeiro momento, pode parecer totalmente inofensivo e inocente muitas vezes, mas que pode representar riscos significativos para a Segurança da Informação: tirar prints ou fotos de tela e compartilhá-los em plataformas públicas ou privadas ou mesmo em Redes Sociais e aplicativos de mensagens.

Ao tirar um simples print de tela, muitas vezes são capturadas informações consideradas sensíveis como:

- Dados pessoais de clientes, colaboradores ou fornecedores;
- Informações confidenciais da empresa;
- Senhas ou credenciais de acesso;
- Informações sobre softwares, sistemas operacionais; e
- Detalhes de projetos internos, e-mails ou documentos importantes.

Assim sendo, tirar um print de tela e um posterior compartilhamento inadvertido pode resultar em:

- Exposição de dados confidenciais e violação de políticas de privacidade;
- Riscos de engenharia social, onde atacantes utilizam essas informações para realizar golpes ou fraudes;
- Comprometimento da segurança de sistemas e infraestrutura;
- Danos à reputação da empresa, além de possíveis penalidades legais.

Exemplo real:

Em 15 de julho de 2020, o Twitter sofreu um ataque cibernético significativo, onde hackers comprometeram cerca de 130 contas de alto perfil, incluindo as de figuras públicas como Joe Biden, Barack Obama e Elon Musk. Os atacantes utilizaram engenharia social para obter acesso a ferramentas administrativas internas do Twitter, permitindo-lhes alterar configurações de contas e publicar tweets em nome dos proprietários. Durante o ataque, os hackers promoveram um golpe de bitcoin, solicitando que seguidores enviassem criptomoedas com a promessa de duplicação. Esse incidente resultou em danos à reputação da plataforma e levantou sérias preocupações sobre a segurança das informações pessoais e corporativas.

Fonte:

- 2020 Twitter account hijacking - Wikipedia

Este exemplo ilustra como o compartilhamento de informações sensíveis, como prints de tela de ferramentas administrativas, pode ser explorado por cibercriminosos para comprometer a segurança de plataformas e dados pessoais.

Para evitar tais riscos, é fundamental que todos os colaboradores estejam cientes da importância de proteger informações confidenciais e sigam as orientações de segurança estabelecidas pela empresa | organização.

A fim de evitar esses riscos, sugerimos que sigam as seguintes orientações:

- Evite tirar prints de telas que contenham informações confidenciais ou sensíveis;
- Caso seja necessário compartilhar uma tela internamente, certifique-se de que as informações sensíveis estejam ocultas ou removidas;
- Após a utilização do print, é importante deletá-lo do dispositivo; e
- Nunca publique prints de tela nas redes sociais ou compartilhe com pessoas de fora da empresa | organização sem a devida autorização.

A colaboração de todos é essencial para garantir a Segurança da Informação. Contamos com a sua atenção e comprometimento!

Atenciosamente,

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Segurança da Informação - Proteja suas informações bancárias

1 mensagem

'sac Serviço de Atendimento ao Cliente' via Segurança da Informação - CIJUN 11 de março de 2025
<segurancainformacao@jundiai.sp.gov.br> às 09:30
Responder a: sac Serviço de Atendimento ao Cliente <sac@cijun.sp.gov.br>
Cco: segurancainformacao@jundiai.sp.gov.br

CLIQUE AQUI

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de segurança para contas Gov.br

1 mensagem

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 14 de março de 2025 às 06:51
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Para: colaboradores@cijun.sp.gov.br
Cco: funcionarios-pmj@jundiai.sp.gov.br

CIJUN
Companhia de Informática de Jundiaí

Prezados(as),

Dicas de segurança para contas *Gov.br*

A plataforma unificada de serviços do Governo Federal para os cidadãos brasileiros (**Gov.br**) foi, de acordo com um estudo da Similarweb, a página de categoria governo mais acessada do mundo. São aproximadamente 164 milhões de usuários cadastrados, acesso a 4,5 mil serviços públicos digitais, mostrando a importância e, claro, notoriedade da plataforma. Ela funciona como um ponto de referência para os diversos ministérios e órgãos que compõem a administração pública federal, e por isso deve ser acompanhada por medidas de segurança extra por parte dos usuários.

Pensando nisso, seguem abaixo algumas dicas de como aumentar a segurança da sua conta:

1. ***Ativar a verificação em duas etapas (duplo fator de autenticação)*** : É importante salientar que a verificação em duas etapas tem como objetivo adicionar uma camada extra de proteção à sua conta, impedindo assim acessos não autorizados, mesmo que sua senha tenha sido comprometida. Abaixo seguem os passos para sua ativação :

a. Abra o aplicativo Gov.br no seu dispositivo (Android | iOS);
b. Acesse sua conta normalmente;
c. No menu inicial, role a tela para baixo e selecione a opção “Segurança da conta”;
d. Escolha a opção “Verificação em duas etapas”;
e. Confirmar a seleção em “Habilitar verificação em duas etapas”; e
f. Desse momento em diante, toda vez que você acessar a conta, será necessário inserir um código gerado no aplicativo Gov.br.

2. ***Limitar o acesso somente para dispositivos autorizados :*** essa opção estando ativa, somente libera acesso ao **Gov.br** de dispositivos previamente aprovados por você. Abaixo seguem os passos para sua ativação :

a. Acesse o aplicativo Gov.br e faça o login;
b. No Menu “Segurança da conta”, selecione a opção “Gerenciar Dispositivos”;
c. Ative a opção “Habilitar acesso apenas para dispositivos autorizados; e
d. Confirme a alteração para bloquear acessos de dispositivos não autorizados.

Caso necessite verificar quais dispositivos têm acesso à sua conta, acesse a opção “Gerenciar dispositivos” e remova qualquer dispositivo que lhe pareça suspeito.

3. ***Habilitar o login com biometria no seu dispositivo :*** O login com biometria permite que somente você acesse sua conta no Gov.br. Abaixo seguem os passos para sua ativação :

a. Acesse o aplicativo Gov.br e entre na sua conta;
b. Selecione o item “Menu”; e
c. Selecione a opção “Ativar login com biometria do celular”

Além das configurações avançadas de segurança citadas acima, seguem abaixo outras dicas não menos importantes :

- ***Utilize senhas fortes e exclusivas :*** senhas com ao menos 8 dígitos, utilizando caracteres alfanuméricos, etc. Nunca utilize senhas simples como por exemplo “12345678” e não reutilize uma senha que você utiliza em outros serviços;
- ***Nunca compartilhe sua senha :*** sua conta Gov.br é pessoal e intransferível, portanto jamais forneça seus dados a desconhecidos, ou qualquer terceiro;
- ***Evite acessar sua conta em dispositivos públicos ou compartilhados :*** dispositivos de terceiros podem armazenar suas credenciais; e
- ***Mantenha seus dados de contato sempre atualizados :*** para receber notificações de login suspeitas e redefinir sua senha, por exemplo, em caso de uma emergência.

Com as dicas acima, você reduz drasticamente os riscos de acessos indevidos na sua conta e também protege suas informações pessoais. Em caso de alguma atividade suspeita, é importante tentar evidenciar, registrar um Boletim de Ocorrência e entrar em contato com os canais de atendimento oficiais do Gov.br.

Fontes :

Como aumentar a segurança da sua conta Gov.br

Como deixar minha conta do Gov.br mais segura? - IT Forum

Atenciosamente,

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Proteja os dados dos destinatários: Use CCO no envio de e-mails

1 mensagem

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 4 de abril de 2025 às 07:46
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Cco: funcionarios-pmj@jundiai.sp.gov.br

CIJUN Companhia de Informática de Jundiaí

Prezadas(os),

Olá!

Você sabia que ao enviar e-mails para múltiplos destinatários sem utilizar a Cópia Oculta (CCO), os endereços de e-mail ficam expostos para todos os recipientes? Essa prática pode gerar riscos de privacidade.

✉️ O que é CCO?

CCO (Cópia Oculta) é um campo do e-mail que permite enviar mensagens a vários destinatários sem que eles vejam os endereços uns dos outros.

✅ Por que usar CCO?

- Protege a privacidade dos destinatários, evitando exposição indevida.
- Reduz riscos de vazamento de informações e uso indevido dos e-mails.
- Demonstra responsabilidade e boas práticas no envio de comunicações corporativas.

📌 Como utilizar corretamente?

1. Ao redigir um novo e-mail, insira seu próprio endereço no campo "Para".
2. Insira todos os destinatários no campo "CCO" (Cópia Oculta).
3. Escreva sua mensagem e envie com segurança!

🔒 A privacidade dos dados é um compromisso de todos! Adote essa prática no seu dia a dia e ajude a fortalecer a proteção de informações.

Atenciosamente,

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Segurança da Informação - Proteja-se contra Vishing

1 mensagem

'sac Serviço de Atendimento ao Cliente' via Segurança da Informação - CIJUN 4 de fevereiro de 2025
<segurancainformacao@jundiai.sp.gov.br> às 09:30
Responder a: sac Serviço de Atendimento ao Cliente <sac@cijun.sp.gov.br>
Cco: segurancainformacao@jundiai.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

🎯 Boas práticas no uso do computador no ambiente de trabalho

1 mensagem

'Ciber Segurança' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 12 de maio de 2025 às 09:11
Responder a: Ciber Segurança <ciberseguranca@cijun.sp.gov.br>
Cco: funcionarios-pmj@jundiai.sp.gov.br

CIJUN
Companhia de Informática de Jundiaí

Prefeitura de Jundiaí

Claudia George Musseli Cezar <ccezar@jundiai.sp.gov.br>

Dicas de segurança: senha forte

1 mensagem

'Comunicação CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 3 de junho de 2025 às 08:00
Responder a: Comunicação CIJUN <comunicacao@cijun.sp.gov.br>
Para: Colaboradores CIJUN <colaboradores@cijun.sp.gov.br>, funcionarios-pmj@jundiai.sp.gov.br

Comunicação
www.cijun.sp.gov.br

Gmail

Pesquisar e-mail

Mail

Chat

Meet

Escrever

Caixa de entrada 1

Com estrela

Adiados

Programados 1

Mais

Marcadores

Curriculos

Mensagens anteriores_DR

Dicas de segurança: Vazamento de dados

Caixa de entrada ×

'Comunicação CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br>
para funcionarios-pmj

Traduza para o português

Comunicação
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de segurança: Limpeza Digital

1 mensagem

'SAC - Serviço de Atendimento ao Cliente CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 24 de junho de 2025 às 08:00
Responder a: SAC - Serviço de Atendimento ao Cliente CIJUN <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

Este é um email automático, não é necessário respondê-lo

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de segurança: Vazamento de dados

1 mensagem

'Comunicação CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 17 de junho de 2025 às 10:51
Responder a: Comunicação CIJUN <comunicacao@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

Comunicação
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de segurança: manter os dispositivos atualizados

1 mensagem

'SAC - Serviço de Atendimento ao Cliente CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 8 de julho de 2025 às 18:11
Responder a: SAC - Serviço de Atendimento ao Cliente CIJUN <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Elizabeth Akiko Araki Oliveira <eoliveir@jundiai.sp.gov.br>

Dicas de segurança: bloquear seu equipamento

1 mensagem

'Comunicação CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br>
Responder a: Comunicação CIJUN <comunicacao@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

22 de julho de 2025 às 08:38

Comunicação
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de Segurança: E-mail suspeito

1 mensagem

'SAC - Serviço de Atendimento ao Cliente CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 5 de agosto de 2025 às 08:00
Responder a: SAC - Serviço de Atendimento ao Cliente CIJUN <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Dicas de segurança: cuidado com o seu crachá

1 mensagem

'SAC - Serviço de Atendimento ao Cliente CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 19 de agosto de 2025 às 08:00
Responder a: SAC - Serviço de Atendimento ao Cliente CIJUN <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Claudia George Musseli Cezar <ccezar@jundiai.sp.gov.br>

Cibersegurança

1 mensagem

'SAC - Serviço de Atendimento ao Cliente CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 2 de setembro de 2025 às 08:00
Responder a: SAC - Serviço de Atendimento ao Cliente CIJUN <sac@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br

S.A.C.
Serviço de Atendimento ao Cliente
www.cijun.sp.gov.br

Prefeitura de Jundiaí

Matheus Bizinotto <mbizinotto@jundiai.sp.gov.br>

Participe da Semana de Cibersegurança 🔒

1 mensagem

'Comunicação CIJUN' via Funcionarios PMJ <funcionarios-pmj@jundiai.sp.gov.br> 6 de outubro de 2025 às 17:01
Responder a: Comunicação CIJUN <comunicacao@cijun.sp.gov.br>
Para: funcionarios-pmj@jundiai.sp.gov.br, Colaboradores CIJUN <colaboradores@cijun.sp.gov.br>

Olá, servidor!

Convidamos você a participar da Semana da Cibersegurança da CIJUN.
A programação contará com especialistas convidados e conteúdos focados na proteção de informações, dados e sistemas, reforçando a importância da segurança digital no nosso dia a dia.

Contamos com sua participação!

SEGURANÇA É UM COMPROMISSO DE TODOS:

SEMANA DE CIBERSEGURANÇA E COMPLIANCE

13/10 - 9h30h às 11h00

Abertura: Michel Domingues, presidente da CIJUN

WorkShop

Privacidade e proteção de dados em foco: entendendo a LGPD

Palestrantes: **Marcelo Fattori**, Presidente da Comissão de Privacidade e Proteção de Dados OAB Jundiaí, e **Daniel Martinelli**, Presidente da OAB Jundiaí

13/10 - 14h às 15h30
WorkShop

LGPD na prática: seus dados, sua privacidade!

Palestrantes: **Marcelo Fattori**, Presidente da Comissão de Privacidade e Proteção de Dados OAB Jundiaí, e **Daniel Martinelli**, Presidente da OAB Jundiaí

Auditório do Paço Municipal

16/10 - 9h30h às 11h00
WorkShop

Cibersegurança

Palestrante: Fabio Aparecido Odoni, Data Protection Officer - Motiva (Grupo CCR)

16/10 - 14h às 15h30
WorkShop

Cibersegurança

Palestrante: Hildemar Baldan, CIJUN

17/10 - 9h30 às 11h0
Roda de conversa

Comunicação
www.cijun.sp.gov.br

Prefeitura de Jundiaí capacita servidores durante a ‘Semana de Cibersegurança e Compliance’ promovida pela CIJUN

Publicada em 14/10/2025 às 17:00

A Prefeitura de Jundiaí, por meio da CIJUN (Companhia de Informática de Jundiaí), promove nesta semana a “Semana de Cibersegurança e Compliance”, com o objetivo de capacitar e conscientizar os servidores municipais sobre a importância da proteção de dados, da segurança digital e do uso responsável das novas tecnologias, como a inteligência artificial.

Capacitação de servidores durante a “Semana de Cibersegurança e Compliance”

O evento é conduzido por especialistas da CIJUN e representantes de instituições parceiras, como a Ordem dos Advogados do Brasil (OAB) Jundiaí, Grupo CCR, entre outros.

De acordo com o presidente da CIJUN, Michel Domingues, a proposta da ação é reforçar o papel essencial do servidor público como elo entre o sistema e o cidadão.

> *“A CIJUN é um pilar estratégico nas áreas de cibersegurança e compliance. Nosso objetivo é conscientizar os servidores de que eles são parte fundamental da segurança da informação. Temos ferramentas tecnológicas avançadas, mas a proteção também depende da conduta e da atenção de quem as utiliza. Em tempos de inteligência artificial e LGPD, é essencial garantir que o uso das tecnologias não exponha dados sensíveis dos cidadãos”, destacou.*

O presidente da OAB Jundiaí, Daniel Martinelli, ressaltou o papel social da instituição na difusão do conhecimento jurídico e na formação de uma cultura de responsabilidade digital. “A OAB tem uma premissa muito importante, que é a função social da Ordem. Entendemos que disseminar informações sobre direitos digitais e proteção de dados é uma forma de contribuir com a sociedade. A parceria com a Prefeitura e a CIJUN reforça nosso compromisso com a ética e com a segurança jurídica nos ambientes público e privado”, afirmou.

Já o presidente da Comissão de Privacidade e Proteção de Dados da OAB Jundiaí, Marcelo Fattori, destacou a importância de um ambiente seguro para o tratamento de informações pessoais, especialmente no setor público.

“O objetivo é promover entre os servidores a compreensão sobre a Lei Geral de Proteção de Dados e a responsabilidade que cada um tem em zelar pelas próprias informações e pelas do cidadão. Garantir a segurança dos dados é essencial para a prestação de serviços públicos de forma responsável e pautada na lei. Quando isso não acontece, há riscos tanto para o cidadão quanto para a administração pública. Nosso papel é justamente fortalecer um ambiente seguro para todos”, explicou.

Assessoria de Imprensa
Fotos: Fotógrafo PMJ

Link original: https://jundiai.sp.gov.br/noticias/2025/10/14/prefeitura-de-jundiai-capacita-servidores-durante-a-semana-de-ciberseguranca-e-compliance-promovida-pela-cijun/