CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

Esta cartilha foi criada para você entender e adotar as práticas de segurança da informação necessárias para proteger seus dados e os da Prefeitura da Cidade do Rio de Janeiro

PREFEITURA RIO | Casa Civil | Transformação Digital e Cidade Inteligente | IplanRio

Prefeito
Eduardo da Costa Paes

Vice-Prefeito
Eduardo Cavaliere

Secretário Municipal da Casa Civil
Leandro Matieli

Subsecretária de Transformação Digital e Cidade Inteligente
Raquel Gonçalves Coimbra Flexa

Diretor Presidente da Empresa Municipal de Informática IPLANRIO
João Carabetta

Grupo de Trabalho
Antônio Sergio de Oliveira Luiz
Bruno Rainho Mendonça
Eduardo Felipe dos Santos Curvelo
Karen Brêda Amaral Lopez
Marcelo Simões Oehrling
Sergio Santos de Jesus

Designer Gráfico
Rodrigo Müller

Versão
V1.0

Data
09/10/2025

Descrição
Cartilha de Segurança da Informação

PREFEITURA RIO

CARTILHA DE
SEGURANÇA DA INFORMAÇÃO 2

Índice:

1. Apresentação

Esta cartilha foi criada para ajudar você a entender e adotar práticas de segurança da informação. Nosso objetivo é garantir que todos os dados da Prefeitura da Cidade do Rio de Janeiro (PCRJ) estejam protegidos.

Queremos simplificar a **Política de Segurança da Informação (PSI)** da PCRJ, tornando-a mais fácil de entender. Quando falamos em "Segurança da Informação", estamos nos referindo a documentos (físicos ou digitais), e-mails, dados pessoais, senhas e informações confidenciais. Todos nós – servidores, gestores e funcionários terceirizados – somos responsáveis por garantir a segurança desses dados.

Lembre-se do ataque hacker que a Prefeitura sofreu em 2022. Aquele incidente aconteceu por causa de uma falha na segurança da informação, provavelmente causada por um usuário que clicou em um link suspeito em um e-mail. Isso paralisou vários serviços da Prefeitura por semanas, afetando a vida de muitos cidadãos.

Para evitar que isso aconteça novamente, a PCRJ criou a PSI, que estabelece regras e responsabilidades para proteger nossas informações. A PSI visa reduzir o risco de novos ataques, mantendo nossas informações seguras, disponíveis e corretas.

A segurança cibernética é um trabalho contínuo. Proteger as informações envolve todo o ciclo de vida dos dados: coleta, armazenamento, processamento, compartilhamento e eliminação.

Esta cartilha oferece dicas básicas para que todos os usuários da rede da Prefeitura possam contribuir para um ambiente mais seguro.

2. Por que a Segurança da Informação é importante?

Hoje em dia, as informações são essenciais para todas as organizações. Proteger essas informações é vital para a sobrevivência de qualquer empresa ou governo. No Município, a segurança das informações é crucial para garantir que os serviços prestados aos cidadãos sejam eficientes e eficazes.

Uma das principais formas de proteger as informações é adotar uma política de segurança da informação. A PSI da Prefeitura do Rio estabelece regras e responsabilidades para resguardar a disponibilidade, integridade, confidencialidade e autenticidade das informações. Além disso, a PSI protege os dados que sustentam todas as atividades da Prefeitura.

Links associados:

- **DECRETO RIO N.º 53700 DE 8 DE DEZEMBRO DE 2023**
  Institui a Política de Segurança da Informação - PSI, com Competências e Responsabilidades

- **RESOLUÇÃO CVL Nº 216 DE 15 DE DEZEMBRO DE 2023**
  Regulamenta as diretrizes da Política de Segurança da Informação – PSI

Escaneie os QR Codes com a câmera do seu celular e acesse os links

3. Conceitos Fundamentais

Quando falamos em segurança, pensamos em proteção. A segurança da informação protege as informações, garantindo que elas permaneçam confidenciais, íntegras e disponíveis.

3.1 Que características da informação devem ser protegidas?

A segurança da informação tem como objetivo preservar **três princípios básicos**:

Confidencialidade:

Garantir que apenas pessoas autorizadas tenham acesso às informações.

- Toda informação deve ser protegida de acordo com seu nível de sigilo, permitindo que apenas as pessoas certas a acessem e usem.

Integridade:

Garantir que as informações não sejam alteradas ou danificadas sem autorização.

- Toda informação deve ser mantida exatamente como foi disponibilizada pela pessoa autorizada.

Disponibilidade:

Garantir que as informações estejam sempre acessíveis quando necessário.

- Toda informação deve estar disponível para os usuários sempre que precisarem.

3.2. Política de Segurança da Informação da PCRJ

A PSI estabelece as regras que orientam todas as ações relacionadas à segurança das informações da Prefeitura.

A PSI garante que as informações municipais estejam protegidas de acordo com sua importância, contribuindo para que os serviços prestados aos cidadãos sejam eficazes.

Para atingir esses objetivos, a PSI:

- **Apresenta as regras de segurança de forma clara e simples.**
- **Define quem é responsável por cada tarefa relacionada à segurança da informação.**
- **Deve ser conhecida por todos os servidores.**

As seções a seguir destacam as regras e responsabilidades descritas na Política de Segurança da Informação da PCRJ.

I. Diretrizes:

- As informações são de propriedade do Município, e os órgãos e entidades municipais são responsáveis por protegê-las contra alterações, destruição ou divulgação não autorizada.

- As informações devem ser classificadas de acordo com sua confidencialidade, integridade e disponibilidade, e devem ser identificadas para que possam ser acessadas, usadas, armazenadas, transportadas e descartadas corretamente.

- As medidas de segurança devem ser proporcionais à importância da informação e ao nível de risco a que ela está exposta.

- Os riscos às informações do município devem ser identificados e tratados regularmente.

- Todas as responsabilidades relacionadas à segurança da informação devem ser claramente definidas e comunicadas.

- Servidores públicos, prestadores de serviço e estagiários devem garantir o sigilo das informações a que tiverem acesso, tomando cuidado com sua divulgação interna e externa.

- As tarefas nos sistemas de informação da PCRJ devem ser distribuídas entre diferentes servidores ou setores, como uma boa prática para mitigação de riscos.

II. Controle de acesso:

- Cada servidor ou pessoa autorizada deve ter uma identificação única, pessoal e intransferível, sendo responsável por todas as atividades realizadas com essa identificação.

- O acesso às informações deve ser limitado ao mínimo necessário para que os usuários possam realizar suas tarefas.

- Prestadores de serviço devem ter acesso com prazo limitado ao período de execução de suas atividades.

III. Capacitação:

- Todos os servidores e prestadores de serviço devem ter o conhecimento mínimo necessário para realizar suas tarefas de forma segura e eficaz, e devem conhecer as políticas e normas de segurança da informação da PCRJ.

- Os servidores devem receber treinamento em segurança da informação para entender as políticas, normas e melhores práticas, e para cumprir suas responsabilidades na proteção das informações da PCRJ.

- Existem normas de segurança da informação complementares à PSI que tratam de temas específicos. É fundamental que todos os servidores da PCRJ leiam essas normas com atenção. ***Repositório das Normas***

Escaneie o QR Code com a câmera do seu celular ou clique para acessar o conteúdo

4. Pílulas do Conhecimento

4.1. Proteção contra Códigos Maliciosos

Códigos maliciosos, como worms, vírus e ransomware, são uma ameaça constante para a segurança das informações. Vamos entender o que são esses códigos e como nos proteger.

I. O que são Códigos Maliciosos?

- **Worms:** Programas que se espalham sozinhos entre os computadores de uma rede.

- **Vírus:** Programas que se copiam e causam danos, precisando de um programa para funcionar.

- **Ransomware:** Bloqueia o acesso aos seus dados (como o ataque sofrido pela PCRJ em 2022).

II. Medidas de Segurança

- **Instalação de Proteções:** Todos os equipamentos devem ter programas de segurança instalados e atualizados.

- **Prevenção de Infecções:** Não baixe arquivos de fontes desconhecidas e verifique sempre os pendrives antes de usá-los.

- **Ações em Caso de Infecção:** Desconecte o equipamento da rede imediatamente e entre em contato com o setor de **Tecnologia da Informação e Comunicação (TIC)** através do ***Iplanfácil***.

Escaneie o QR Code com a câmera do seu celular ou clique para acessar o conteúdo

III. Competências e Responsabilidades

- **Órgãos e Entidades:**
  - Garantir que todos os equipamentos estejam de acordo com as normas de segurança.
  - Assegurar que as áreas de TIC administrem soluções de proteção eficazes.

- **Gestão de TIC:**
  - Pesquisar, implementar e administrar soluções de proteção contra códigos maliciosos.
  - Garantir que os equipamentos estejam executando as soluções de proteção corretamente e que estas estejam atualizadas.
  - Planejar e gerenciar riscos relacionados a códigos maliciosos.
  - Prover tratamento de incidentes e homologar soluções de proteção.

- **Usuários:**
  - Verificar se os programas de proteção estão ativos e atualizados antes de usar os equipamentos.
  - Relatar imediatamente (Iplanfácil) qualquer suspeita de ataque por código malicioso.
  - Seguir as práticas de segurança e não alterar as configurações de proteção sem autorização.

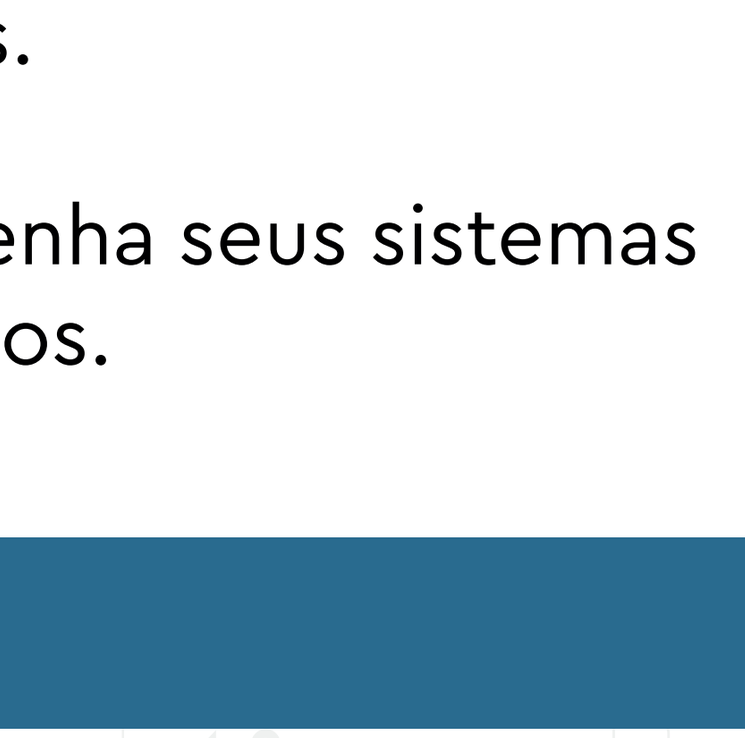
IV. Conclusão

A proteção contra códigos maliciosos é uma responsabilidade de todos. **Ao seguir as orientações desta cartilha, você contribuirá para um ambiente digital mais seguro.**

- **Verificação Constante:** Verifique sempre se os programas de proteção estão ativos e atualizados.
- **Cuidados com E-mails:** Não abra anexos ou links de remetentes desconhecidos.
- **Atualizações Regulares:** Mantenha seus sistemas e aplicativos sempre atualizados.

4.2. Uso da Internet

A Internet é muito importante para a Prefeitura, ajudando a melhorar os serviços oferecidos aos cidadãos. No entanto, é preciso usar a Internet de forma segura e eficiente.



I. Recomendações para uso adequado da internet

- **Suporte ao Trabalho:** A Internet deve ser usada principalmente para o trabalho.

- **Restrições:** Não use a Internet para acessos que não tenha autorização.

- **Verificação de Sites:** **Verifique se os sites são seguros** (p.ex: cadeado fechado na barra de endereços), especialmente ao fazer transações importantes.

A conexão é segura

- **Certificados Digitais:** Verifique se os sites têm certificados digitais para garantir a segurança, como o "**https://**" no endereço e o cadeado fechado na barra de endereços.

II. Competências e Responsabilidades

- **IplanRio:** Administra o serviço de Internet, garantindo segurança e funcionalidade.

- **Usuários:** Devem seguir as práticas seguras de uso da Internet estabelecidas pela PSI e normas complementares.

III. Conclusão

Fique atento às atualizações de segurança e participe de programas de conscientização para usar a Internet de forma segura e eficiente.

- Cabe ressaltar que todos os acessos à Internet realizados dentro da rede corporativa podem ser monitorados para garantir a segurança.

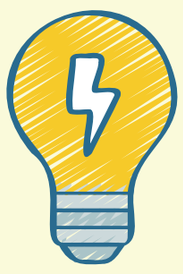
4.3. Uso de Correio Eletrônico

O correio eletrônico é muito importante para a comunicação na Prefeitura. Vamos aprender como usá-lo de forma segura e responsável.

I. Das Contas de Correio Eletrônico

- **Uso Pessoal e Intransferível:** Cada conta deve ser usada apenas pela pessoa a quem pertence, e essa pessoa é responsável por tudo o que fizer com a conta.

- **Criação e Gestão de Contas:** As contas são controladas pelos gestores de acesso, que cuidam da criação, atualização e exclusão das contas.



DICA:
Use senhas fortes e diferentes para sua conta de e-mail e nunca as compartilhe.

II. Recomendações para uso adequado do Correio Eletrônico

- **Gerenciamento de Mensagens:** Limpe sua caixa de entrada, apagando mensagens desnecessárias.

- **Segurança da Informação:** Evite clicar em links suspeitos e verifique os anexos antes de abri-los. Sempre que possível, ative a autenticação em duas etapas **(autenticação multifator – MFA)**, que adiciona uma camada extra de segurança para acessar sua caixa postal. Veja como ativá-la no QR Code ao lado.

Escaneie o QR Code com a câmera do seu celular

Escaneie o QR Code com a câmera do seu celular ou clique para acessar o conteúdo

III. Competências

- **IplanRio:** Responsável pela gestão técnica e suporte do serviço de correio eletrônico, no caso de endereço nome@prefeitura.rio.

- **Órgãos e Entidades:** Devem manter os inventários de usuários atualizados e registrar movimentações.

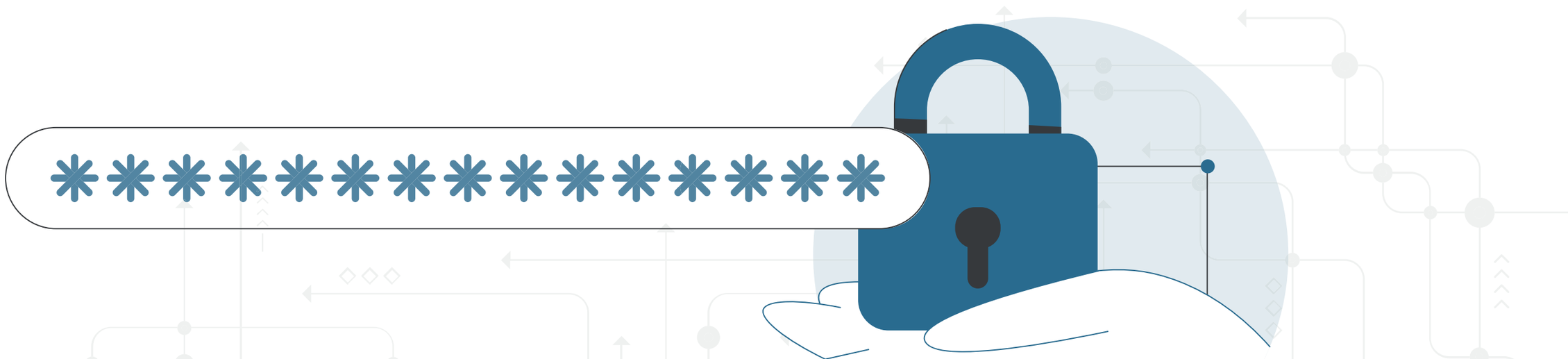
- **Usuários:** Devem seguir as normas e práticas seguras de uso do Correio Eletrônico.

IV. Conclusão

O uso correto do correio eletrônico corporativo é fundamental para a segurança e eficiência das operações na Administração Pública. Ao seguir as diretrizes apresentadas nesta cartilha, você contribuirá para um ambiente de trabalho mais seguro e produtivo.

4.4 Senhas

As senhas ainda são um dos principais mecanismos para autenticação em sistema de informação e serviços digitais. Com isso torna-se crucial a adoção de boas práticas no suporte a sua criação e manutenção visando a proteção do seu sigilo.



I. Recomendações para Criação e Manutenção de Senhas

Proteção de Senhas

- **Confidencialidade:** Mantenha suas senhas em segredo. Não as compartilhe.

- **Alteração Regular:** Mude suas senhas regularmente, especialmente se suspeitar de comprometimento.

- **Armazenamento Seguro:** Nunca escreva suas senhas em papéis ou use o recurso de armazenamento automático de senhas em navegadores.

- **Atualização:** As senhas devem ser alteradas a cada 60 dias.

- **Uso de Senhas**

- **Complexidade:** As senhas devem conter letras maiúsculas, minúsculas, números e caracteres especiais. Exemplo: "**S3gur@2025!**".

- **Tamanho Mínimo:** Senhas de acesso devem ter pelo menos 10 caracteres, enquanto senhas administrativas devem ter no mínimo 14.

- **Criação e Atualização:**
  A senha inicial é temporária e deve ser alterada no primeiro acesso.

II. Dicas:

- **Pense em uma frase de grande significado;**
- **Componha uma estrutura de formação própria;**
  - Minhas senhas irão começar com um caractere especial;
  - Os demais caracteres serão as 1ªs letras de cada palavra da frase;
  - Os números presentes na frase serão expressos de forma completa;
  - Minhas senhas sempre terminarão com letras maiúsculas.
- **Componha a senha a partir da estrutura de formação;**
- **Memorize a frase e a estrutura de formação;**
- **Nunca revele suas senhas;**
- **Construa senhas fortes;**
- **Troque suas senhas periodicamente;**
- **Nunca permaneça com senhas temporárias;**
- **Ativar a autenticação em duas etapas (autenticação multifator (MFA). Essa medida adiciona uma camada extra de segurança, exigindo uma segunda forma de verificação além da senha, que pode ser para outra conta de e-mail, ou por mensagem SMS. Veja como ativá-la no QR Code ao lado.**

Escaneie o QR Code com a câmera do seu celular ou clique para acessar o conteúdo

III. Conclusão

As senhas são amplamente usadas para controlar o acesso às aplicações municipais. A quebra de sua confidencialidade pode permitir acessos não autorizados, expondo a Administração Pública a riscos de segurança da informação. Assim, torna-se fundamental sua proteção conforme as recomendações desta cartilha.

4.5. O que é Phishing?

Phishing é um tipo de golpe em que pessoas mal-intencionadas tentam enganar você para conseguir suas informações pessoais, como senhas, números de cartão de crédito ou outros dados importantes. Esse golpe normalmente acontece por meio de mensagens falsas, enviadas por e-mail, SMS, redes sociais ou outros aplicativos, que parecem confiáveis, mas na verdade são armadilhas.

Como o golpe acontece no dia a dia?

No dia a dia, o phishing costuma aparecer assim:

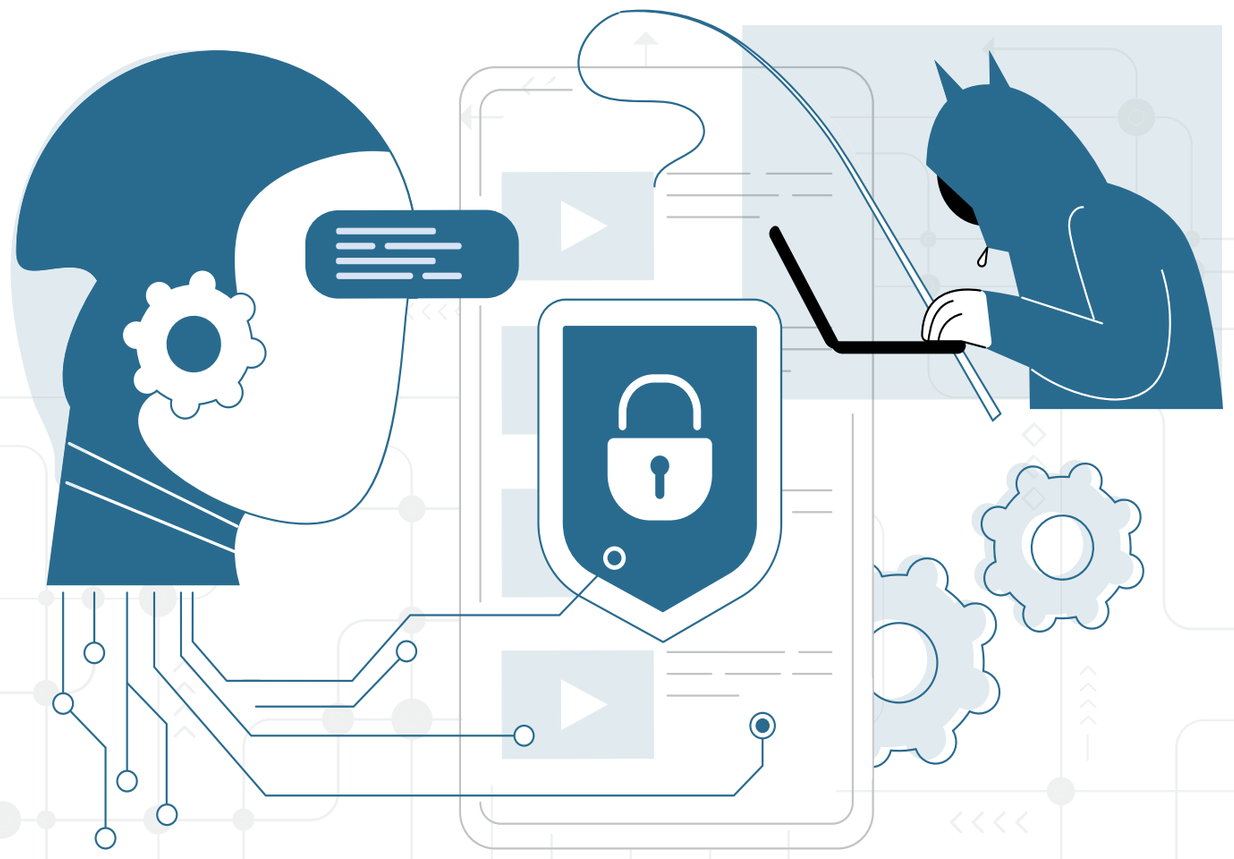
- Você recebe um e-mail dizendo que sua conta do banco vai ser bloqueada se você não clicar em um link e preencher seus dados.
- Uma mensagem chega pelo WhatsApp, aparentemente de uma loja famosa, oferecendo um prêmio ou promoção irresistível, pedindo para você clicar num site e preencher um cadastro.
- Um SMS informa que há uma encomenda para você, com um link para "acompanhar a entrega", exigindo que você forneça informações pessoais.

Essas mensagens geralmente tentam assustar, pressionar ou atrair você com ofertas boas demais para serem verdade.

Dicas rápidas para identificar tentativas de phishing

Veja alguns sinais de alerta para identificar esse tipo de golpe:

- **Erros de português:** mensagens com muitos erros de escrita ou frases estranhas.
- **Urgência suspeita:** ameaças de bloqueio imediato da sua conta ou pedidos para agir rápido.
- **Links estranhos:** endereço do site diferente do oficial, com nomes esquisitos ou letras trocadas.
- **Solicitação de dados pessoais:** pedidos para informar senha, número de cartão ou código enviado por SMS.
- **Ofertas boas demais:** promoções e prêmios que parecem exagerados ou impossíveis.
- **Dica importante:** Se ficar em dúvida, não clique em links nem forneça seus dados. Entre em contato diretamente com a empresa ou pessoa pelo canais oficiais para checar a veracidade da mensagem.



5. Observações e Recomendações Finais

- **Verificação Constante:** Sempre verificar se as soluções de proteção estão ativas e atualizadas.

- **Cuidados com E-mails:**
  - Não abrir anexos ou links de remetentes desconhecidos;
  - Atenção a e-mails com erros de português ou formatação incomum, pois podem ser sinais de phishing;
  - Verificar o endereço de e-mail do remetente para garantir que é legítimo e não uma imitação; e
  - Não fornecer informações confidenciais (como senhas ou dados bancários) por e-mail. Empresas legítimas geralmente não solicitam esse tipo de informação por essa via.

- **Atualizações Regulares:** Manter sistemas e aplicativos sempre atualizados.

- **Educação Contínua:** Participar de treinamentos regulares sobre segurança da informação.

- **Monitoramento Constante:** Utilizar ferramentas de monitoramento para detectar rapidamente qualquer anomalia.

- **Mantenha-se informado:** Conheça as normas de segurança e as siga rigorosamente.

- **Reporte Incidentes:** Notifique imediatamente qualquer problema com os equipamentos **(IPLANFÁCIL)**.

- **Aplicação das Normas:** As normas são aplicáveis a todos os agentes públicos e devem ser seguidas rigorosamente.

- **Sanções:** Violações das normas podem resultar em sanções administrativas.

Ficou com alguma dúvida?

Entre em contato com a

Subsecretaria de Transformação Digital e Cidade Inteligente

transformacaodigital@prefeitura.rio

Escaneie o QR Code com a câmera do seu celular ou clique para acessar o contato

PREFEITURA

RIO

Casa Civil

Transformação Digital e Cidade Inteligente

IplanRio