UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

DICAS DE SEGURANÇA

A UNIPRIME se preocupa com a sua segurança ao usar nossos serviços, e por isso elaboramos estas recomendações práticas e objetivas, para que você se proteja e não seja vítima de fraudes e golpes aplicados em meios digitais.

FISHING

O que é *Fishing*?

O *Fishing*, conhecido também como *Phishing* ou *Phishing-scam* é um tipo de fraude por meio da qual um golpista se passa por uma pessoa ou mesmo uma empresa confiável para obter **dados pessoais e financeiros** da vítima.
Na maioria das vezes, a vítima é induzida a clicar em um determinado link e/ou preencher dados para que **o golpista tenha acesso às informações.**

Exemplos de *Fishing:*

E-mails com títulos indicando pendências de pagamento com a alegação que a não regularização pode acarretar graves consequências; ou envio de mensagens com a promessas de recebimento de prêmios em dinheiro onde o resgate só ocorre mediante **cadastro de informações pessoais** no link indicado na mensagem.

Há casos em que a mera abertura da mensagem ou e-mail já faz com que os **dados sejam automaticamente roubados**. Com acesso às informações, o golpista usa os dados da vítima para acessar uma conta, criar outras identidades, contrair empréstimos, realizar algum outro tipo de crime utilizando-se dos dados da vítima, ou mesmo para vendê-los a outras pessoas.

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

SMISHING

O que é Smishing?

O *Smishing* é uma forma de *Fishing* realizada por meio de envio de mensagens de texto – **"SMS"**, utilizando nomes de empresas conhecidas. A mensagem na maioria das vezes possui um **link para que a vítima forneça dados pessoais**.

Exemplos de *Smishing:*

Uma prática muito utilizada pelos golpistas é o envio de mensagens de texto intituladas como "PROMOÇÃO IMPERDÍVEL" ou "OFERTA", ou mesmo ameaças de cobrança de determinado serviços. O objetivo desse tipo de mensagem é **roubar os seus dados através de link malicioso** ou mesmo pelo simples fato de clicar na mensagem.

Como se proteger de *Fishing* ou *Smishing*?

- Não abra mensagens de e-mail de destinatários desconhecidos; mensagens com assuntos estranhos ou chamativas ou mensagens direcionadas à caixa de Spam;
- Verifique sempre se o remetente do e-mail é conhecido ou se você já teve contatos anteriores. Muitos criminosos utilizam-se de e-mails com erros gramaticais ou com formatos diferentes, como a inclusão de números ou alternância de letras maiúsculas e minúsculas;
- Evite baixar arquivos automaticamente ou aceitar solicitações de *downloads* que não sejam de fato necessários para o uso do site;
- Não execute arquivos que não tenham sido solicitados pelo site, pois *softwares* maliciosos, como *Malwares*, podem acessar suas informações

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

- pessoais e enviá-las automaticamente para criminosos do outro lado da rede;
- Certifique-se que seu sistema operacional e antivírus estão atualizados;

Atenção: A Uniprime não envia e-mails, SMS, mensagens de WhatsApp, nem realiza ligações solicitando dados pessoais ou informações financeiras sigilosas. Em caso de dúvidas quanto à idoneidade de mensagens ou ligações recebidas, entre em contato imediatamente com sua agência e informe seu gerente. Os contatos estão disponíveis em https://www.uniprime.com.br/agencias.

Fui vítima de *Fishing* ou de *Smishing*, e agora?

Caso você tenha sido vítima de *Fishing* ou de *Smishing*, tome imediatamente as seguintes providências:

1. Guarde cópia da mensagem, e-mail ou qualquer outro documento relacionado;
2. Reporte a fraude à Delegacia de Polícia de Crimes Virtuais mais próxima e às empresas que possam ter tido suas contas/acessos utilizados;
3. Desconecte todos os seus dispositivos e troque todas as senhas antigas por novas que preferencialmente nunca tenham sido utilizadas;
4. Utilize sempre seu antivírus e escaneie seus dispositivos por completo em busca de vírus;
5. Mantenha-se informado e fique alerta sempre que receber alguma mensagem ou e-mail suspeitos, assim, menor será a probabilidade de seus dispositivos serem infectados novamente.

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

GOLPE DO BOLETO FALSO

O que é o golpe do "boleto falso"?

Nesse tipo de golpe, o golpista falsifica boletos de compras ou mesmo cobranças e enviam às vítimas normalmente por e-mail ou SMS. Os remetentes forjados são muito semelhantes aos de empresas reais, o que faz o boleto parecer confiável. O código de barras do boleto é modificado para que o dinheiro seja enviado para a conta do golpista.

Como evitar o golpe?

- **Desconfie** de boletos enviados sem qualquer solicitação prévia;
- A UNIPRIME envia boletos somente através de seus **canais oficiais**;
- A UNIPRIME **não** encaminha boletos por WhatsApp;
- **Desconfie** de boletos com dificuldade de reconhecimento pela leitora de código de barras;
- **Confira** os dados do cedente (beneficiário) como Nome, CNPJ, Banco, Dados Bancários. É importante também conferir os dados do pagador;
- Sempre que estiver em dúvida sobre a veracidade e procedência do boleto, entre em **contato com a UNIPRIME por meio dos canais oficiais**.

Paguei um boleto falso, e agora?

Mantenha preservadas as evidências que mostram como o criminoso entrou em contato e como o boleto falso chegou até você;
Com esses documentos, procure a Delegacia de Polícia mais próxima ou faça um Boletim de Ocorrência Eletrônico.

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

GOLPES PELO WHATSAPP

Acesso ou clonagem da conta no WhatsApp

Aplicativos de mensagem instantânea também são utilizados para prática de golpes. Uma das técnicas usadas pelos golpistas para a **clonagem do WhatsApp** é o envio de promoções ou oportunidades falsas, mediante a solicitação de um **"código de confirmação"** por meio de SMS. Esse código é a chave de acesso à conta pessoal do WhatsApp, o que permite ao criminoso acessar ou clonar a conta da vítima. A fraude também pode ocorrer por meio da criação de **contas falsas**, com o uso do nome e foto da vítima.

Com acesso aos dados da vítima, os golpistas enviam mensagens aos contatos e solicitam depósitos, empréstimos, em nome da vítima. Além disso, o fraudador pode ter acesso às suas conversas e outros dados que podem ser base para novos golpes e prejuízos.

Como evitar golpes no WhatsApp?

- Ative a **"Confirmação em duas etapas"** no seu WhatsApp. No app, acesse: Configurações>Conta>Confirmação em duas etapas>Ativar. Veja como ativar: https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=pt_br.
- Ajuste a **privacidade da sua foto de perfil no WhatsApp** para que apenas seus contatos salvos possam visualizá-la. No app, acesse: Configurações>Conta>Privacidade>Foto do perfil: selecione "Meus contatos" ou "Ninguém";
- Nunca informe o código de verificação recebido por SMS no seu celular, para ninguém;
- Baixe apenas aplicativos de confiança e não envie informações pessoais para desconhecidos;

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

- Desconfie de ofertas muito vantajosas, nas quais basta enviar um código para ganhar descontos, brindes entre outras vantagens;
- Desconfie de pessoas pedindo dinheiro com urgência. Nestes casos, ligue para a pessoa que pediu o dinheiro e confirme se realmente é quem você conhece;
- Desconfie de contatos que dizem ter trocado de número de celular repentinamente.

Minha conta foi invadida ou clonada, e agora?

1. Alerte seus contatos para desconsiderarem o número clonado ou a conta falsa, assim que souber do golpe ou o mais rápido possível;
2. Envie e-mail para support@whatsapp.com relatando o ocorrido. Siga as instruções para resgatar a conta ou informar sobre a conta falsa;
3. Com informações e evidências do ocorrido, procure uma Delegacia de Polícia ou faça um **Boletim de Ocorrência Eletrônico**;
4. **Se o fraudador se fez passar pela UNIPRIME, entre em contato por meio de nossos canais oficiais e reporte o fato.**

ENGENHARIA SOCIAL

Há diversos golpes que usam técnicas de manipulação psicológica para convencer a vítima de que está em contato com uma pessoa ou empresa, quando na verdade está em contato com um golpista.

Exemplos de engenharia social:

- página na internet ou rede social falsas ou muito parecidas com a página oficial de uma empresa ou instituição para que as vítimas insiram dados pessoais e dados financeiros;

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

- contatos via telefone fazendo ofertas, passando-se por central de telefonia. Assim, quando a vítima faz um pagamento através destes meios, acaba pagando ao golpista;
- contatos via telefone informando a necessidade da troca do cartão de crédito e envio de portador que fará a retirada do cartão.

Como evitar golpes de engenharia social?

1. Verifique se você está em um site ou aplicativo **oficial da instituição**.
2. Leia atentamente as informações do site, pois sites fraudulentos costumam conter erros de português ou configurações visuais desajustadas.
3. Verifique se a página contém **Termos de Uso e/ou Políticas de Privacidade** indicando o CNPJ da empresa.
4. **Verifique se o site é seguro**. Procure por comentários sobre o site na internet.
5. Ao acessar qualquer site, verifique se há o símbolo de um cadeado ao lado do endereço (URL). Ao clicar no símbolo do cadeado, aparecerão informações sobre o certificado de segurança do site.

DICAS PARA SE PREVENIR CONTRA GOLPES

Indicamos abaixo algumas recomendações do que **NUNCA** fazer:

- **Nunca forneça os dados, senha da sua conta, a ninguém;**
- **Nunca use senhas fracas, como datas de aniversário;**
- **Nunca informe o código de verificação recebido por SMS no seu celular, para ninguém;**

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

- **Nunca abra ou responda e-mails ou mensagens de pessoas desconhecidas ou de conteúdo duvidoso ou muito chamativo.**

O que **SEMPRE** fazer:

- **Sempre entre em contato com a UNIPRIME por meio de nossos canais oficiais;**
- **Sempre use senhas fortes e guarde elas em segurança;**
- **Sempre ative a verificação de duas etapas no seu WhatsApp;**
- **Sempre limite quem pode ver sua foto de perfil nas redes sociais;**
- **Sempre desconfie de ofertas excessivamente baratas ou vantajosas;**
- **Sempre mantenha seu programa de antivírus atualizado;**
- **Sempre guarde um backup dos seus arquivos mais importantes;**

COMO A UNIPRIME ENTRA EM CONTATO COMIGO?

A UNIPRIME e seus funcionários nunca realizam ligações ativas para solicitação de dados pessoais ou financeiros ou mandam mensagens privadas em redes sociais/WhatsApp.

Assim, somente as comunicações feitas pelos canais indicados abaixo devem ser consideradas oficias:

Telefone
Os números oficiais de nossas agências podem ser consultados através do link: https://www.uniprime.com.br/agencias

Site Oficiai
https://www.uniprime.com.br/

UNIPRIME CENTRAL
Tel.: 43 3305.2900
Av. Higienópolis, 1044 • Centro
CEP 86020-080 • Londrina/PR
www.uniprime.com.br

Caso você saiba de qualquer movimentação suspeita, entre em contato com a UNIPRIME diretamente com o seu gerente.

Proteja-se! As ações preventivas são sempre muito eficientes para que você não seja vítima de uma fraude ou golpe digital.