FORK the Banks

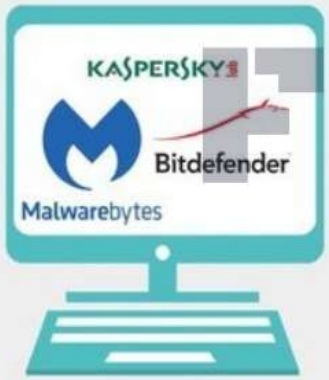
Guia de Segurança

Os Ativos Digitais estão criando uma revolução mundial. É importante garantir que seus ativos permaneçam protegidos. **Por favor, use este guia para ajudar a manter seus ativos seguros.**

Só compre e troque Ativos Digitais de um PC ou dispositivo limpo e atualizado. Por favor, execute um **protetor de malware** e um **scanner de antivírus** e um **firewall**. Atualize diariamente.

Use senhas muito fortes com pelo menos 15 a 20 caracteres. Os **gerenciadores de senhas** ajudam a rastrear essas senhas. Os gerenciadores de senha de armazenamento local são preferidos.

Gestão de Senhas



Malware and Antivírus Protection

Autenticação móvel não é segura. Com este método de recuperação de senha, os representantes de serviço ao cliente do seu telefone celular geralmente são projetados e o **cartão SIM** pode ser portado. Ligue para sua operadora de telefonia celular para adicionar uma **NÃO PORTA** e nenhum encaminhamento de chamadas para sua conta. Você pode estar sujeito a **ataques SS7**. A recuperação do SMS é de sua responsabilidade.

No topo das senhas, autenticação de dois fatores **(2FA)** é importante. Faça o download de um aplicativo em um dispositivo e certifique-se de anotar cada senha secreta ao adicionar um website. O **Google Authenticator**, FreeOTP e o **Authy** são os preferidos.

A autenticação de hardware **(Fido)** é ainda mais segura. Use isso em cima de gerenciadores de senhas ou onde estiver disponível.

Autenticação de dois fatores

Os **ataques de phishing** são uma das ameaças mais comuns aos Ativos Digitais. A adição de **HTTPs** em qualquer lugar do seu navegador pode ajudar a detectar sites maliciosos.

Alterar seu DNS pode filtrar ataques de phishing e sites falsificados. Use **Quad9, OpenDNS** ou o **DNS público do Google** para adicionar outra camada de proteção. Alguns servidores DNS registram temporariamente, mas o **Quad9** não.

Como um nível extra de proteção. use uma **VPN** que não registre dados privados. Use uma VPN, especialmente quando você não está na sua rede doméstica.

Contas de Email

O **ProtonMail aceita criptografia e privacidade com seriedade**. As contas são **grátis** para criar e você pode ter quantas quiser. Não é uma má ideia ter várias contas de email. Nunca use um email que tenha sido afetado por uma **violação de dados** ou por um email que você usa para **redes sociais**

Privacidade e Segurança do Navegador

Ativos Digitais não devem ser deixados em uma exchanger a menos que você esteja negociando ativamente. O **armazenamento a frio** é o método mais seguro de armazenar suas chaves privadas. As **carteiras de papel** são melhores para longo prazo, mas as **carteiras de hardware** são convenientes. **Carteiras quentes e carteiras desktop** onde você tem controle de suas **chaves privadas** são as melhores. Faça backup de suas **carteiras e armazene suas** senha de recuperação em local à prova d'água e fogo.

Seja seu próprio banco. Seja sua própria segurança.

Armazenamento de Chaves

EXODUS

keepkey

TREZOR

electrum