CO2 Trade

SECURITY

CO2 Trade Ltda.

51.450.220/00001-58

São Paulo - Brasil

PT-BR / EN-US / ES

Rev. 1

Boas práticas de segurança

Última atualização: 20 de dezembro de 2023.

As principais práticas de segurança na Web para transações financeiras e compras de ativos:

Proteger suas informações financeiras em atividades online é crucial, principalmente ao usar computadores e celulares. Aqui estão algumas práticas essenciais de segurança na web para manter seu dinheiro e ativos seguros:

1. Práticas Gerais:

1.1. Senhas fortes: use senhas exclusivas e complexas (mais de 12 caracteres) com uma mistura de letras maiúsculas e minúsculas, números e símbolos. Evite informações pessoais como datas de nascimento e nomes de parentes, pets e palavras de dicionário. Use um gerenciador de senhas para armazenamento seguro.

1.2. Autenticação multifator (MFA): habilite a MFA sempre que possível e disponível. Isso adiciona uma camada extra de segurança além das senhas, geralmente usando um código enviado via sms ao seu telefone ou e-mail.

1.3. Atualizações de software: mantenha seus sistemas operacionais, navegadores e aplicativos atualizados com os patches de segurança mais recentes. Software desatualizado é vulnerável a ataques.

1.4. Cuidado com o phishing: nunca clique em links ou anexos suspeitos, mesmo de remetentes aparentemente familiares. Verifique os endereços dos sites diretamente, não por meio de links.

1.5. Conexões Seguras: Procure por “https” no endereço do site e um símbolo de cadeado para garantir conexões criptografadas. Evite fazer transações financeiras em redes Wi-Fi públicas como de aeroportos, cafeterias e restaurantes.

1.6. Antivírus e antimalware: use software antivírus e antimalware confiável e mantenha-os atualizados. Verifique seus dispositivos regularmente em busca de ameaças.

1.7. Cuidado com a engenharia social: os golpistas podem tentar manipular você para que revele informações pessoais. Tenha cuidado com ligações, e-mails ou mensagens não solicitadas, especialmente

Good security practices

Last updated: December 20, 2023.

Top web security practices for financial transactions and asset purchases:

Protecting your financial information in online activities is crucial, especially when using computers and cell phones. Here are some essential web security practices to keep your money and assets safe:

1. General Practices:

1.1. Strong passwords: Use unique, complex passwords (12+ characters) with a mix of upper and lower case letters, numbers, and symbols. Avoid personal information such as dates of birth and names of relatives, pets and dictionary words. Use a password manager for secure storage.

1.2. Multi-factor authentication (MFA): Enable MFA whenever possible and available. This adds an extra layer of security on top of passwords, usually using a code sent via SMS to your phone or email.

1.3. Software updates: Keep your operating systems, browsers, and applications up to date with the latest security patches. Outdated software is vulnerable to attacks.

1.4. Beware of phishing: never click on suspicious links or attachments, even from seemingly familiar senders. Check website addresses directly, not through links.

1.5. Secure Connections: Look for “https” in the website address and a padlock symbol to ensure encrypted connections. Avoid making financial transactions on public Wi-Fi networks such as airports, cafes and restaurants.

1.6. Antivirus and antimalware: Use reputable antivirus and antimalware software and keep them updated. Check your devices regularly for threats.

1.7. Beware of social engineering: Scammers may try to manipulate you into revealing personal information. Be careful with unsolicited calls,

Buenas practicas de seguridad

Última actualización: 20 de diciembre de 2023.

Principales prácticas de seguridad web para transacciones financieras y compras de activos:

Proteger su información financiera en actividades en línea es crucial, especialmente cuando usa computadoras y teléfonos celulares. A continuación se presentan algunas prácticas de seguridad web esenciales para mantener seguros su dinero y sus activos:

1. Prácticas Generales:

1.1. Contraseñas seguras: utilice contraseñas únicas y complejas (más de 12 caracteres) con una combinación de letras mayúsculas y minúsculas, números y símbolos. Evite información personal como fechas de nacimiento y nombres de familiares, mascotas y palabras del diccionario. Utilice un administrador de contraseñas para un almacenamiento seguro.

1.2. Autenticación multifactor (MFA): habilite MFA siempre que sea posible y esté disponible. Esto agrega una capa adicional de seguridad además de las contraseñas, generalmente utilizando un código enviado por SMS a su teléfono o correo electrónico.

1.3. Actualizaciones de software: mantenga sus sistemas operativos, navegadores y aplicaciones actualizados con los últimos parches de seguridad. El software obsoleto es vulnerable a los ataques.

1.4. Tenga cuidado con el phishing: nunca haga clic en enlaces o archivos adjuntos sospechosos, ni siquiera de remitentes aparentemente familiares. Verifique las direcciones de los sitios web directamente, no a través de enlaces.

1.5. Conexiones seguras: busque "https" en la dirección del sitio web y un símbolo de candado para garantizar conexiones cifradas. Evite realizar transacciones financieras en redes Wi-Fi públicas como aeropuertos, cafeterías y restaurantes.

1.6. Antivirus y antimalware: utilice software antivirus y antimalware de buena reputación y manténgalos actualizados. Revise sus dispositivos con regularidad en busca de amenazas.

1.7. Tenga cuidado con la ingeniería social: los estafadores pueden intentar manipularlo para que revele información personal. Tenga cuidado con las llamadas, correos electrónicos o mensajes no

aquelas que oferecem ganhos financeiros rápidos. Tenha bastante atenção para quais dados estão visíveis em suas redes sociais.

2. Transações financeiras e compras de ativos:

2.1. Escolha sites confiáveis: use apenas sites confiáveis com um forte histórico de segurança e atendimento ao cliente. Verifique análises online e certificações de segurança.

2.2. Revise as políticas do site: Leia a política de privacidade, cookies e os termos de uso do serviço do site antes de fazer qualquer transação. Entenda como seus dados são coletados, usados e protegidos.

2.3. Métodos de pagamento robustos: use métodos de pagamento seguros, como links de pagamento onde o cliente é direcionado para a plataforma bancária e depois da transação realizada com sucesso, retorna par ao site original. Estes sistemas possuem proteção contra fraudes e normalmente são plataformas de pagamento online verificadas. Verifique se o pagamento realizado está sendo enviado realmente para a empresa indicada, cheque números de registro, nomes e marcas.

2.4. Verificação de transações: verifique todas as transações e atividades da conta regularmente. Esteja alerta para atividades suspeitas e comunique imediatamente quaisquer irregularidades.

2.5. Proteja seus dispositivos: use senhas ou PINs fortes para bloquear seu computador e telefone. Ative recursos de bloqueio automático e considere aplicativos de segurança para proteção adicional.

2.6. Cuidado com dispositivos públicos: evite fazer transações financeiras ou acessar informações confidenciais em computadores públicos ou dispositivos compartilhados.

2.7. Sair e limpar histórico: Sempre saia de contas financeiras e sites após o uso. Limpe seu histórico de navegação e cache regularmente para remover informações confidenciais. O uso de guias e abas anônimas ajuda, porém não são 100% eficazes.

2.8. Monitore seus extratos bancários e faturas de cartão de crédito: monitore regularmente seus relatórios em busca de atividades não autorizadas. Considere opções de congelamento de conta e cancelamento de senhas e cartões para proteção extra.

2.9. Horários comuns: dê preferência para realizar transações em horário comercial normal e movimentações de maior valor dentro do

emails or messages, especially those offering quick financial gains. Pay close attention to what data is visible on your social networks.

2. Financial transactions and asset purchases:

2.1. Choose reputable sites: Only use reputable sites with a strong track record of security and customer service. Check online reviews and security certifications.

2.2. Review the site's policies: Read the site's privacy policy, cookies policy, and terms of service before making any transaction. Understand how your data is collected, used and protected.

2.3. Robust payment methods: use secure payment methods, such as payment links where the customer is directed to the banking platform and, after a successful transaction, returns to the original website. These systems have fraud protection and are usually verified online payment platforms. Check that the payment made is actually being sent to the indicated company, check registration numbers, names and brands.

2.4. Transaction Verification: Check all transactions and account activities regularly. Be alert to suspicious activity and immediately report any irregularities.

2.5. Secure your devices: Use strong passwords or PINs to lock your computer and phone. Enable auto-lock features and consider security apps for additional protection.

2.6. Be careful with public devices: Avoid making financial transactions or accessing confidential information on public computers or shared devices.

2.7. Log out and clear history: Always log out of financial accounts and websites after use. Clear your browsing history and cache regularly to remove sensitive information. Using anonymous tabs and tabs helps, but they are not 100% effective.

2.8. Monitor your bank statements and credit card statements: Regularly monitor your reports for unauthorized activity. Consider account freezing options and canceling passwords and cards for extra protection.

2.9. Common hours: give preference to carry out transactions during normal business hours and transactions of higher value within banking

solicitados, especialmente aquellos que ofrecen ganancias financieras rápidas. Presta mucha atención a qué datos son visibles en tus redes sociales.

2. Transacciones financieras y compras de activos:

2.1. Elija sitios de buena reputación: utilice únicamente sitios de buena reputación con un sólido historial de seguridad y servicio al cliente. Consulte reseñas en línea y certificaciones de seguridad.

2.2. Revise las políticas del sitio: lea la política de privacidad, la política de cookies y los términos de servicio del sitio antes de realizar cualquier transacción. Comprenda cómo se recopilan, utilizan y protegen sus datos.

2.3. Métodos de pago sólidos: utilice métodos de pago seguros, como enlaces de pago donde se dirige al cliente a la plataforma bancaria y, después de una transacción exitosa, regresa al sitio web original. Estos sistemas tienen protección contra fraude y suelen ser plataformas de pago online verificadas. Verifique que el pago realizado realmente esté siendo enviado a la empresa indicada, verifique números de registro, nombres y marcas.

2.4. Verificación de transacciones: verifique todas las transacciones y actividades de la cuenta con regularidad. Esté alerta a actividades sospechosas e informe inmediatamente cualquier irregularidad.

2.5. Proteja sus dispositivos: use contraseñas o PIN seguros para bloquear su computadora y teléfono. Habilite las funciones de bloqueo automático y considere aplicaciones de seguridad para obtener protección adicional.

2.6. Tenga cuidado con los dispositivos públicos: evite realizar transacciones financieras o acceder a información confidencial en computadoras públicas o dispositivos compartidos.

2.7. Cerrar sesión y borrar historial: cierre siempre sesión en cuentas financieras y sitios web después de su uso. Borre su historial de navegación y su caché con regularidad para eliminar información confidencial. Usar pestañas y pestañas anónimas ayuda, pero no son 100% efectivos.

2.8. Supervise sus extractos bancarios y de tarjetas de crédito: supervise periódicamente sus informes para detectar actividades no autorizadas. Considere opciones de congelación de cuentas y cancelación de contraseñas y tarjetas para mayor protección.

2.9. Horario común: da preferencia para realizar transacciones en horario comercial normal y transacciones de mayor valor dentro del

horário bancário, assim em caso de falha poderá ter um suporte e atendimento para correção mais rápido e eficiente.

3. Segurança para celulares:

3.1. Baixe aplicativos apenas de lojas oficiais: baixe aplicativos apenas de lojas de aplicativos oficiais, como Google Play ou Apple App Store. Evite fontes de terceiros, sites online ou arquivos APK.

3.2. Revise as permissões do aplicativo: revise cuidadosamente as permissões do aplicativo antes de fazer o download. Conceda acesso apenas às funções necessárias para o funcionamento do aplicativo.

3.3. Desativar serviços de localização: desative os serviços de localização, a menos que esteja usando ativamente aplicativos que os exijam. Isso reduz o risco de rastreamento e violações de dados.

3.4. Use VPNs para Wi-Fi público: considere usar uma VPN verificada e contratada para conexões seguras ao usar Wi-Fi público, especialmente para transações financeiras. Serviços de VPN gratuitos ou promocionais oferecem o mesmo perigo de redes abertas ou até mesmo piores.

3.5. Relate problemas de segurança: se você encontrar qualquer atividade suspeita ou preocupação de segurança, relate-a imediatamente ao site ou à instituição financeira.

Lembre-se de que a segurança online é um processo contínuo. Seguindo essas práticas e permanecendo vigilante, você pode reduzir significativamente o risco de fraude financeira e roubo de ativos ao usar sites para transações financeiras e compra de ativos.

4. Contate-nos

Se você tiver alguma dúvida sobre esta guia, entre em contato conosco em info@co2trade.org.

FIM.

hours, so in the event of a failure you can have faster and more efficient support and correction service.

3. Mobile Security:

3.1. Download apps only from official stores: Download apps only from official app stores such as Google Play or Apple App Store. Avoid third-party sources, online websites, or APK files.

3.2. Review app permissions: Carefully review app permissions before downloading. Grant access only to functions necessary for the application to function.

3.3. Turn off location services: Turn off location services unless you're actively using apps that require them. This reduces the risk of tracking and data breaches.

3.4. Use VPNs for public Wi-Fi: Consider using a verified and contracted VPN for secure connections when using public Wi-Fi, especially for financial transactions. Free or promotional VPN services offer the same danger as open networks or even worse.

3.5. Report security issues: If you encounter any suspicious activity or security concerns, report them to the website or financial institution immediately.

Remember that online security is an ongoing process. By following these practices and remaining vigilant, you can significantly reduce the risk of financial fraud and asset theft when using websites for financial transactions and asset purchases.

4. Contact us

If you have any questions about this guide, please contact us at info@co2trade.org.

END.

horario bancario, así en caso de falla podrás tener un servicio de soporte y corrección más rápido y eficiente.

3. Seguridad móvil:

3.1. Descargue aplicaciones solo de tiendas oficiales: descargue aplicaciones solo de tiendas de aplicaciones oficiales como Google Play o Apple App Store. Evite fuentes de terceros, sitios web en línea o archivos APK.

3.2. Revisar los permisos de la aplicación: revise cuidadosamente los permisos de la aplicación antes de descargarla. Otorgue acceso solo a las funciones necesarias para que la aplicación funcione.

3.3. Desactive los servicios de ubicación: desactive los servicios de ubicación a menos que esté utilizando activamente aplicaciones que los requieran. Esto reduce el riesgo de seguimiento y violaciones de datos.

3.4. Utilice VPN para Wi-Fi público: considere utilizar una VPN verificada y contratada para conexiones seguras cuando utilice Wi-Fi público, especialmente para transacciones financieras. Los servicios VPN gratuitos o promocionales ofrecen el mismo peligro que las redes abiertas o incluso peores.

3.5. Informe problemas de seguridad: si encuentra alguna actividad sospechosa o problemas de seguridad, infórmelo al sitio web o a la institución financiera de inmediato.

Recuerde que la seguridad en línea es un proceso continuo. Si sigue estas prácticas y permanece alerta, puede reducir significativamente el riesgo de fraude financiero y robo de activos al utilizar sitios web para transacciones financieras y compras de activos.

4. Contáctanos

Si tiene alguna pregunta sobre esta guía, contáctenos en info@co2trade.org.

FIN.

Este documento foi redigido em português brasileiro, e traduzido automaticamente para inglês e espanhol. Qualquer falha de interpretação deverá ser reanalisada sobre o texto original em português.

This document was written in Brazilian Portuguese, and automatically translated into English and Spanish. Any error in interpretation must be re-analyzed using the original Portuguese text.

Este documento fue escrito en portugués brasileño y traducido automáticamente al inglés y español. Cualquier error de interpretación deberá ser analizado nuevamente utilizando el texto original en portugués.


CO2
Trade