Roteiro Comunicado aos Clientes

19.4646.1 – PSAP – Grupo Plural

Contato PROOF
Miguel Reis - miguel.reis@proof.com.br
Adrielle Silva - adrielle.silva@proof.com.br
Kenzo Osanai - kenzo.osanai@proof.com.br

Contato GRUPO PLURAL
Anderson Mendes – anderson.mendes@genialinvestimentos.com.br
Karina Voss - karina.voss@genialinvestimentos.com.br

Data de emissão
25-03-2020

TODOS OS DIREITOS RESERVADOS PROOF SERVIÇOS E COM. DE INF. LTDA ®
O logotipo PROOF é marca comercial registrada da PROOF SERVIÇOS E COM. DE INF. LTDA. Todas as demais marcas, logotipos e produtos pertencem aos seus respectivos proprietários. Com exceção do expressamente definido neste documento, este material, na íntegra ou partes dele, não pode ser copiado, reproduzido, distribuído, republicado, apresentado, anunciado ou transmitido de nenhuma maneira ou por nenhum meio, incluindo, mas não limitado a meios eletrônicos, mecânicos, de fotocópia, de gravação ou de qualquer outra índole, sem a permissão prévia por escrito da PROOF SERVIÇOS E COM. DE INF. LTDA ou do titular dos direitos autorais.

Roteiro dos Comunicados aos Clientes

19.4646.1 – PSAP – Grupo Plural

Sumário

Histórico de Mudanças

Versão	Data	Modificado por	Mudança
1.0	17-03-20	Miguel Reis	Documento original.

1) SEGURANÇA DA INFORMAÇÃO É PRIORIDADE NA GENIAL

Você pode ficar tranquilo que seus dados estão seguros conosco.

Dica #01: Você sabe o que é Account Takeover?

Account Takeover são **roubos de identidade** que ocorrem frequentemente com o objetivo de acessar contas online. É possível identificar essas tentativas em uma **sequência de situações incomuns, como o recebimento de mais e-mails ou SMS confirmando compras debitadas em sua conta ou realizadas com o seu cartão**. Em seguida, o recebimento de mais e-mails ou mensagens.

Aqui, na Genial Investimentos, nossas plataformas passam por constantes atualizações de segurança, com o objetivo de prestar o melhor nível de serviço aos nossos clientes. Mas saiba que você também precisa estar muito atento ao uso de suas credenciais de acesso.

Dica: nunca utilize o mesmo usuário/senha para acessar a nossa plataforma em outros serviços na internet.

Dica #02: Atenção com mídias removíveis desconhecidas.

Uma técnica simples e bastante efetiva utilizada por criminosos chama-se baiting, que consiste no uso de uma isca - em geral, uma mídia removível infectada com um arquivo malicioso - para se infiltrar em um ambiente digital de uma empresa ou roubar credenciais da vítima para, assim, ter acesso a informações privilegiadas

Dica #03: Atenção com suas senhas!

A técnica de shoulder surfing, também conhecida como “espiada por cima do ombro”, é bem comum no espaço de trabalho e, principalmente, em ambientes públicos (cafeterias, transporte público, restaurantes etc.). Preste sempre atenção se ao seu redor não há nenhuma outra pessoa por perto que possa ver a sua tela.

Dica #04: Atenção com atualização e instalação de softwares.

Sempre estar com as atualizações em dia torna mais difícil que cibercriminosos explorem vulnerabilidades de softwares e sistemas desatualizados. Além disso, sempre escolha baixar

aplicativos em seu dispositivo pelas lojas oficiais, como o Google Play, a App Store e a Microsoft Store.

Dica #05: Atenção com o antivírus no smartphone!

Engana-se quem pensa que não é necessário se preocupar com a segurança digital do smartphone. Devido à grande popularidade desses dispositivos, eles são alvo de ataques constantemente. Por isso, não deixe de instalar o antivírus, assim, você evita que arquivos maliciosos sejam executados no seu dispositivo móvel.