Conheça as principais medidas de segurança que o BTG Pactual implementa para a proteção das informações de seus clientes:

A estratégia de defesa cibernética do BTG Pactual está estruturada de forma a garantir que a estrutura de defesa evolua continuamente, em velocidade compatível com o desenvolvimento dos riscos e ameaças cibernéticos, aumentando a nossa resiliência a ataques e diminuindo nossas vulnerabilidades.

Os objetivos da estratégia de defesa cibernética do BTG Pactual são:

Identificar

- Identificar todos os ativos de tecnologia e classificá-los em função de sua relevância para o negócio;
- Acompanhar a evolução dos riscos e ameaças cibernéticas para orientar e priorizar ações de defesa.

Proteger:

- Desenvolver continuamente a cultura de segurança cibernética no BTG Pactual;
- Reduzir nossas vulnerabilidades para assegurar a manutenção de um nível adequado de segurança;
- Proteger a confidencialidade, a integridade e a acessibilidade das informações.

Detectar:

- Monitorar os ativos digitais para identificar eventos de segurança.

Responder e Recuperar:

- Responder com eficácia a incidentes de segurança;
- Assegurar que o BTG Pactual se recupere tempestivamente de incidentes;
- E evoluir nossas defesas a partir das lições aprendidas com os incidentes.

Dessa forma, a estrutura de defesa cibernética do BTG Pactual evolui conforme os riscos das áreas de negócios. Os dados de nossos funcionários e clientes estão seguros com todos os mecanismos utilizados para a sua proteção.

Saiba o que você pode fazer para tornar sua experiência mais segura

Cuidado com suas senhas

Ainda que seja o meio mais comum de autenticação, muitas pessoas ainda não conhecem os riscos de ter suas senhas comprometidas. Caso alguém tenha acesso às suas senhas, essa pessoa pode enviar mensagens se passando por você, ter acesso às suas informações, ter acesso ao seu histórico de mensagens e prejudicar a segurança dos seus dados. A seguir, listamos as melhores práticas para você gerenciar suas senhas:

- Não compartilhe as suas senhas com ninguém. Suas senhas são utilizadas em serviços assinados por você e, portanto, devem servir apenas para esse uso.
- Tenha senhas complexas. Utilize sempre a combinação mais complexa possível e, caso o sistema permita, utilize caracteres especiais, letras maiúsculas combinadas com minúsculas e números.
- Não utilize informações pessoais ou que sejam fáceis de descobrir em suas senhas, como data de nascimento, nome dos filhos, data de nascimento dos filhos, número de telefone, etc.
- Troque sua senha com frequência: pelo menos a cada 90 dias.
- Não use sua senha em diversos sistemas diferentes. O ideal é utilizar uma para cada sistema ou serviço.

- Armazene a sua senha em locais seguros. Não é indicado anotar suas senhas em locais de fácil acesso. Existem ferramentas chamadas de gerenciadores de senha, que permitem que você armazene senhas complexas sem a necessidade de se recordar de todas, sabendo apenas a senha principal do gerenciador.

Proteja seus dispositivos

Nossos dados estão armazenados em sistemas e esses, por sua vez, estão em dispositivos eletrônicos: tablets, celulares, notebooks, entre outros. Esses dispositivos precisam ser protegidos para que fiquem seguros contra criminosos. Você sabe protegê-los?

- Sempre faça as atualizações de segurança solicitadas pelos seus dispositivos o quanto antes. Essas atualizações corrigem falhas que podem ser exploradas por atacantes.
- Tenha um antivírus, caso disponível para o seu sistema operacional. Essa ferramenta procura por vírus no seu dispositivo e corrige essa ameaça.
- Coloque senha para acesso e não a compartilhe com ninguém. Siga as instruções para uso de senha citadas acima.

Cuidado com Engenharia Social

No contexto de segurança da informação, Engenharia Social são técnicas empregadas por criminosos para induzir a vítima a tomar uma ação, como informar dados, clicar em links, realizar transferências de valores, entre outros.

Os principais golpes que envolvem engenharia social são:

- E-mails falsos (phishing). Envio de e-mails falsos genéricos ou direcionados a uma pessoa ou grupo específico.
- Golpes do WhatsApp: fraudadores se passando por você e entrando em contato com outras pessoas ou mesmo “sequestrando” a sua conta do aplicativo.
- Ligações falsas. Criminosos entram em contato se passando por outra pessoa (órgãos do governo ou pesquisa, por exemplo) e fingindo situações para roubar dados.

Muitas dessas tentativas de golpes vão tentar manipular os sentimentos da vítima, com mensagens que demandam ação urgente, que envolvem relações pessoais ou questões financeiras.

Phishing é quando o criminoso envia mensagens aparentemente reais a uma vítima, aguardando que ela tome determinada ação. Hoje a principal porta de entrada de hackers em uma empresa é o phishing. Também é uma maneira fácil de conseguir credenciais válidas de pessoas comuns.

Esses e-mails podem se passar por promoções imperdíveis em lojas conhecidas, bancos (informando operações realizadas, bloqueio de senha, etc), mensagens de sistemas, entre outros, sendo muitas vezes e-mails genéricos, que poderiam ter como alvo qualquer pessoa. São enviados para uma grande quantidade de usuários e, ao cair no phishing, a vítima acaba passando dados confidenciais, credenciais ou mesmo baixando artefatos maliciosos.

Como não ser vítima de phishing?

Sempre que você receber uma mensagem, desconfie se:

- Você desconhece o remetente
- O contato estiver diferente do habitual
- Houver um tom muito impessoal

- Houver um tom de urgência, como “participe agora”, “preciso de ajuda urgente”, etc.

Fique atento!

- Criminosos podem criar e-mails ou sites muito parecidos com um legítimo, trocando ou omitindo algumas letras.
- Se o assunto envolver pagamentos ou resgate valores, sempre se certifique através de outro canal que você realmente está falando com a pessoa certa.
- Se receber uma mensagem suspeita de uma loja, prefira entrar no site pelo navegador (sem clicar em links da mensagem) e verificar se aquela promoção realmente existe ou se foi realmente feita alguma transação em sua conta.