ASPECTOS GERAIS DE SEGURANÇA DA INFORMAÇÃO

À Colaboradores, Parceiros e Agentes envolvidos nas atividades da CREDFRANCO

Versão 02

2023

CREDFRANCO
Grupo Financeiro

Contas e Senhas

Por meio de contas e senhas os sistemas conseguem identificar quem você é! Dessa forma, proteger sua senha é essencial para se prevenir dos riscos envolvidos no uso de sistemas/ internet, pois é o segredo da sua senha que garante a sua identidade.

Caso algum colega de trabalho ou terceiro saiba sua conta de usuário e tenha acesso à sua senha, ele poderá passar-se por você para realizar ações em seu nome.

Os **riscos** caso algum invasor acesse sua conta são:

Acessar seu e-mail e (i) ler e/ou apagar e-mails; (ii) furtar sua lista de contatos e enviar e-mails em seu nome; (iii) enviar mensagem de spam e/ou conteúdo phishing e códigos maliciosos; (iv) pedir reenvio de senha de outras contas.

CREDFRANCO
Grupo Financeiro

Contas e Senhas

Acessar seu computador e (i) apagar seus arquivos e obter informações sensíveis; (ii) instalar códigos e serviços maliciosos.

Acessar sua conta bancária e verificar seu extrato e saldo bancário.

Seja cuidadoso(a) ao criar e gerenciar suas senhas!

CREDFRANCO
Grupo Financeiro

Contas e Senhas

Orientações:

- Evite usar dados pessoas na elaboração de senhas;
- Não exponha suas senhas;
- Não forneça sua senha para outra pessoa, em nenhuma hipótese;
- Evite usar a mesma senha para todos os serviços que você acessa;
- Armazene suas senhas de forma segura;
- Procure reduzir a quantidade de informações que possam ser coletadas sobre você, nossos parceiros ou clientes;
- Seja cuidadoso com as informações que você disponibiliza a terceiros;
- Cadastre uma senha de acesso que seja bem elaborada e complexa (alfanumérica);

Preserve a sua privacidade, os dados da CREDFRANCO, de nossos Clientes e Parceiros !

CREDFRANCO
Grupo Financeiro

Ataques Maliciosos

Códigos maliciosos, também conhecidos como pragas e *malware,* são programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos.

Os equipamentos podem ser infectados caso você:

- Acesse páginas web maliciosas;
- Utilizar pen drive e afins infectados;
- Executar arquivos infectados, obtidos em anexos de mensagens eletrônicas, mídias removíveis, sites, redes sociais e afins.

Após infectar o seu equipamento, o código malicioso pode executar ações como se fosse você, como acessar informações, apagar arquivos, criptografar dados, enviar mensagens e instalar outros códigos maliciosos.

CREDFRANCO
Grupo Financeiro

Ataques Maliciosos

Orientações:

- Mantenha sempre seu antivírus atualizado. Caso verifique alguma inconsistência na sua máquina, **chame o suporte**!
- Seja cuidadoso(a) ao clicar em links;
- Não considere que as mensagens vindas de conhecidos são sempre confiáveis – o campo de remetente do e-mail pode ter sido falsificado;
- Antes de acessar um link curto, procure usar complementos que permitam visualizar o link de destino;

CREDFRANCO
Grupo Financeiro

Incidentes

Incidente é qualquer ação que pode causar a perda ou dano de alguma informação ou ativo, o que traz prejuízos à empresa, em maior ou menor grau. Por isso é tão importante identificar esse tipo de situação com antecedência e garantir a integridade de nossas informações.

Recebeu um e-mail cujo domínio não é @credifranco.com.br ou de origem duvidosa?

Recebeu uma ligação pedindo informações das áreas CREDFRANCO, Clientes ou Parceiros?

Cuidado! Podem ser ataques direcionados!

Caso perceba alguma situação incomum envolvendo a CREDFRANCO, nossos parceiros ou clientes, avise a área de Governança e Compliance e Tecnologia da Informação (TI) por meio do e-mail compliance@credifranco.com.br.

CREDFRANCO
Grupo Financeiro

Segurança da Informação na Prática

Supervírus de computador ataca infraestrutura iraniana

Jonathan Fildes
Repórter de tecnologia da BBC News

23 setembro 2010

O Stuxnet, ao contrário da maioria de viroses, não está conectado com a internet. Ele infecta máquinas Windows por meio de portas USB e pen drives usados para transportar arquivos.

Uma vez que infecta uma máquina da intranet, a rede interna, da empresa, o vírus busca uma configuração específica de um software para controle industrial feito pela Siemens.

CREDFRANCO
Grupo Financeiro

Boas Práticas

Para garantir o acesso seguro, basta se comprometer com alguns **hábitos diários** para a segurança de seus dados:

- Jamais compartilhe suas senhas com outras pessoas, nem anote em locais de fácil acesso;
- Jamais utilize a mesma senha para diferentes sistemas;
- Altere a senha com frequência, a cada 45 dias ou sempre que for solicitado via sistema;
- Lembre-se de se deslogar de sites que peçam suas senhas ao sair deles, como redes sociais e principalmente dos sistemas e serviços da CREDFRANCO;
- Sempre que deixar sua estação de trabalho, mesmo que por um instante, bloqueie a tela do seu computador e evite que outros vejam suas informações;
- Equipamentos fornecidos pela sua empresa são uma concessão e devem ser utilizados somente para fins de trabalho;
- Nunca compartilhe ou salve documentos com informações restritas ou confidenciais em áreas de transferência ou diretório aberto e de uso compartilhado por outros colaboradores e prestadores de serviço;

CREDFRANCO
Grupo Financeiro

Boas Práticas

Quanto ao e-mail, **jamais envie**:

- Suas senhas e outros dados de cadastros, como login;
- Conteúdos, fotos ou vídeos que não tenham relação com seu trabalho;
- Informações sensíveis sem a devida autorização;
- E-mails, anexos ou links que sejam de fontes desconhecidas ou suspeitas;
- E-mails que tenham anexos sem a proteção adequada;
- Mensagens que violem direitos autorais;
- Correntes;

CREDFRANCO
Grupo Financeiro

Dúvidas

Bárbara Fideles
Analista de Compliance
compliance@credifranco.com.br

CREDFRANCO
Grupo Financeiro