INSTITUTO FEDERAL
Minas Gerais

VOLUME 1
AGOSTO/2025

CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

DTI - IFMG

AUTENTICAÇÃO MULTIFATOR (MFA ou 2FA):

O ESCUDO EXTRA QUE VOCÊ PRECISA

Imagine que sua senha é a chave da porta da sua casa. Agora, imagine que, além da chave, você adiciona uma tranca extra e um cadeado. Fica muito mais seguro, certo? Isso é a MFA!

A autenticação multifator (ou "duplo fator de autenticação"), também conhecida pelas siglas em inglês MFA e 2FA, é uma camada extra de segurança. Mesmo que alguém descubra sua senha, não conseguirá acessar sua conta sem o segundo fator, que pode ser um código no celular, uma digital ou um aplicativo autenticador.

Geralmente, os fatores se enquadram em três categorias:

1. **Algo que você sabe:** A sua senha ou um PIN.
2. **Algo que você tem**: Um objeto físico, como seu celular (para receber um código SMS ou usar um app autenticador), um token de segurança ou um cartão.
3. **Algo que você é:** Uma característica sua, única. É a biometria, como sua impressão digital, o reconhecimento facial ou da íris.

Por que é essencial ativar a autenticação multifator?

- **Proteção robusta contra roubo de senhas:** Vazamentos de dados são comuns. Se sua senha vazar de um serviço, criminosos tentarão usá-la em vários outros. Com a MFA, eles serão barrados no segundo passo.
- **Barreira contra ataques de *phishing*:** Mesmo que você seja enganado e digite sua senha em um site falso, o invasor não terá acesso ao seu segundo fator (como seu celular), mantendo a conta segura.
- **Tranquilidade para seus dados:** Garante que apenas você tenha acesso às suas informações pessoais, e-mails, redes sociais, dados financeiros e profissionais.
- **Requisito de segurança moderno:** É uma prática padrão e muitas vezes obrigatória para sistemas importantes, como os de bancos, e plataformas institucionais (como o SEI, Suap e sistemas de e-mail corporativos).

Dica: Não espere! A maioria dos serviços importantes oferece essa proteção. Procure nas configurações de "Segurança" ou "Privacidade" das suas contas e ative a autenticação multifator: e-mail, redes sociais, bancos, sistemas do IFMG... tudo!

COFRE DE SENHAS:

SUA MEMÓRIA AGRADECE

Ainda está usando 'ifmg123' como senha? A gente precisa conversar...

Manter senhas seguras e diferentes para cada serviço é essencial. Mas quem consegue lembrar de tantas? É aí que entra o gerenciador de senhas, também conhecido como cofre de senhas.

Esses aplicativos guardam suas senhas com segurança, criptografadas, e você só precisa lembrar uma senha mestre.

A segurança de todo o seu cofre depende da força da sua **Senha Mestre**. Para ela, siga duas regras de ouro:

- **Seja longa e única:** Não a use em nenhum outro lugar. Crie uma frase que só você conheça (ex: "MinhaPrimeiraCasaEraAmarela!2005") em vez de uma única palavra.
- **Nunca a esqueça:** Como nem a empresa do cofre pode recuperá-la, se você a perder, o acesso ao cofre é perdido para sempre. Guarde-a na sua memória.

Alguns cofres de senhas gratuitos para uso pessoal: **Proton Pass**, **Bitwarden** e **NordPass**

Principais vantagens de usar um cofre de senhas:

✓ **Cria senhas impenetráveis para você**

Chega de usar "senha123" ou o nome do seu cachorro. Os cofres geram senhas longas, aleatórias e extremamente fortes (como G#t7&kP@v!R$zX9) para cada um dos seus sites e serviços.

✓ **Armazena tudo com segurança máxima**

Suas senhas são guardadas de forma criptografada. Isso significa que elas são transformadas em um código complexo e ilegível que só pode ser "traduzido" de volta com a sua Senha Mestre.

✓ **Preenche senhas automaticamente (e com segurança!)**

Além da conveniência de não precisar digitar, o preenchimento automático é um recurso de segurança. Ele ajuda a proteger contra sites de phishing, pois o cofre só sugere preencher a senha no site legítimo e verdadeiro ao qual ela pertence.

✓ **Sincroniza em todos os seus dispositivos**

Precisa da senha do Wi-Fi no celular? Ou da senha do banco no computador? O cofre sincroniza suas informações de forma segura para que você as tenha sempre à mão, onde quer que esteja.

SPAM, PROPAGANDA OU PHISHING?

ENTENDA AS DIFERENÇAS!

Nem todo e-mail indesejado é perigoso - mas alguns são! Vamos descomplicar:

SPAM:

São mensagens em massa, não solicitadas, enviadas para milhares de pessoas ao mesmo tempo. Geralmente são inúteis e podem conter links para produtos duvidosos ou até malwares.

- **Objetivo:** Vender algo de forma massiva ou, no pior caso, espalhar vírus.
- **Exemplos:** "Compre agora o elixir da juventude!", "Fique rico rápido!", "Você ganhou um prêmio incrível!".

E-MAIL DE MARKETING (Propaganda):

São e-mails de empresas e serviços com os quais você já interagiu: cadastrou-se em uma loja, assinou uma newsletter ou comprou um curso. Embora possam lotar sua caixa de entrada, são legítimos.

- **Objetivo:** Manter um relacionamento com o cliente, anunciar promoções e novidades.
- **Exemplos:** "Promoção especial só para você!", "Lançamos uma nova coleção!", "Lembrete: seu carrinho de compras".

Dica: Por lei, todo e-mail de marketing legítimo deve ter um link para "**Cancelar inscrição**" ou "**Descadastrar**", geralmente no rodapé da mensagem.

PHISHING:

Este é o verdadeiro vilão. É uma fraude criada para "pescar" suas informações confidenciais. Os criminosos se passam por uma empresa ou pessoa confiável (seu banco, uma rede social, um órgão do governo) para enganar você e roubar seus dados.

- **Objetivo:** Roubar suas credenciais (usuário e senha), dados de cartão de crédito ou informações pessoais.
- **Fique atento aos sinais:**
  - **Senso de urgência ou ameaça:** "Sua conta será bloqueada em 24h!", "Detectamos uma atividade suspeita, confirme seus dados IMEDIATAMENTE".
  - **Erros de português** ou formatação estranha.
  - **Links falsos:** Passe o mouse sobre o link (sem clicar!) para ver o endereço real. Muitas vezes ele não corresponde ao da empresa.
  - **Remetente suspeito:** O e-mail parece vir do seu banco, mas o endereço é @gmail.com, hotmail.com, ou algo similar.

RECEBEU UM E-MAIL?

VEJA O QUE FAZER:

Se for **Spam** ou **Marketing** indesejado:

NÃO RESPONDA.

Apenas use a opção "**Marcar como Spam**" ou "**Denunciar Spam**" do seu provedor de e-mail.

Para marketing legítimo, use o link de **descadastro** no fim do e-mail.

Se você suspeita que é **Phishing**:

NÃO CLIQUE EM NADA.
NÃO RESPONDA.
NÃO BAIXE ANEXOS.

Encaminhe a mensagem imediatamente para a equipe de segurança do IFMG: **etir@ifmg.edu.br**.

Depois, pode **apagar** o e-mail.

FIQUE ATENTO, SEMPRE!

A segurança da informação é um hábito diário, não só uma campanha. Com pequenas atitudes, você evita grandes dores de cabeça:

- ✓ Ative a autenticação multifator (MFA/2FA).
- ✓ Use um cofre de senhas
- ✓ Desconfie de links e anexos em e-mails estranhos.
- ✓ Mantenha seus aplicativos e sistema operacional atualizados.
- ✓ E, sempre que tiver dúvida, ***fale com a DTI***!