

SEGURANÇA DA INFORMAÇÃO

Internet e Navegação Segura

Cuidados essenciais para navegar com segurança nos ambientes corporativos



A internet é uma ferramenta essencial para o trabalho, mas também é uma das principais portas de entrada para ameaças à segurança da informação. Golpes, sites falsos, downloads maliciosos e redes desprotegidas podem comprometer dados, sistemas e a própria rotina da CAAPSMML.

Por isso, a navegação segura na internet é um dos pilares do Plano de Segurança da Informação da CAAPSMML, elaborado pela Comissão de Segurança da Informação. Pequenos cuidados no dia a dia fazem toda a diferença na proteção das informações institucionais.

FIQUE ATENTO AOS RISCOS MAIS COMUNS



O phishing é uma das fraudes mais frequentes: mensagens e sites falsos que imitam empresas ou órgãos confiáveis para roubar dados e credenciais.

Alguns dos golpes e riscos mais comuns na internet são:

- **Phishing:** e-mails, mensagens ou sites falsos que se passam por instituições confiáveis para roubar senhas e dados pessoais;
- **Sites falsos e clonados:** páginas que imitam serviços legítimos (bancos, órgãos públicos, lojas) para capturar informações;
- **Downloads maliciosos:** arquivos, programas ou anexos infectados com vírus, spyware ou ransomware;
- **Redes Wi-Fi públicas ou desconhecidas:** conexões sem proteção adequada, vulneráveis à interceptação de dados;
- **Anúncios e pop-ups enganosos:** janelas e banners que induzem o clique para instalar softwares indevidos ou redirecionar a páginas fraudulentas.

⚠ Sinais de um site ou mensagem suspeitos

Erros de português, urgência excessiva ("sua conta será bloqueada"), links encurtados, endereços com pequenas variações do nome oficial e solicitações de dados sensíveis são sinais de alerta. Na dúvida, não clique.

BOAS PRÁTICAS DE NAVEGAÇÃO SEGURA



Verificar o endereço e o cadeado de segurança do site é um hábito simples que previne muitos golpes.

Para navegar com mais segurança, adote os seguintes cuidados:

- X** Acesse apenas sites confiáveis e verifique se o endereço começa com "https://" e exibe o ícone de cadeado;
- X** Confira sempre a URL antes de inserir dados ou credenciais, atentando para pequenas alterações no nome do site;
- X** Não clique em links ou anexos recebidos de remetentes desconhecidos ou suspeitos;
- X** Baixe arquivos e programas apenas de fontes oficiais e homologadas pela área de Tecnologia da Informação;
- X** Mantenha o navegador, o antivírus e o sistema operacional sempre atualizados;
- X** Evite acessar sistemas institucionais ou informar dados sensíveis em redes Wi-Fi públicas;
- X** Feche sessões e efetue logout ao término do uso de sistemas e serviços, principalmente em computadores compartilhados;
- X** Utilize apenas dispositivos e equipamentos autorizados pela CAAPSMML para acessar sistemas institucionais.

Antes de clicar, confirme

Recebeu um link ou anexo inesperado, mesmo de um contato conhecido? Confirme por outro canal (telefone, mensagem direta) antes de abrir. Contas podem ser clonadas ou invadidas para espalhar golpes.

REDES PÚBLICAS E DOWNLOADS: ATENÇÃO REDOBRADA



Redes Wi-Fi abertas, disponíveis em aeroportos, cafés e locais públicos, não oferecem garantias de proteção contra interceptação de dados.

Sempre que possível, utilize a rede corporativa ou uma conexão de dados móvel confiável para acessar sistemas e informações da CAAPSMML.

Em caso de suspeita

Se você suspeitar de um site falso, receber uma mensagem fraudulenta em nome da CAAPSMML ou identificar comportamento estranho no computador, comunique imediatamente a área de Tecnologia da Informação e evite continuar a navegação até a verificação.

NAVEGAR COM SEGURANÇA TAMBÉM É PROTEGER A CAAPSMML



Cada acesso consciente à internet reduz os riscos de incidentes de segurança e protege os dados institucionais e dos servidores.

A navegação segura integra as ações de conscientização previstas no Plano de Segurança da Informação da CAAPSMML e contribui para o fortalecimento da cultura de segurança no ambiente institucional.