UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA

Segurança Digital

Guia Rápido

De Navegação Segura na Internet

Panorâma sobre golpes comuns, boas práticas, dicas de segurança e mais.

SETOR DE INFORMÁTICA

(49) 2049-9534
cinf.ceo@udesc.br

SETOR DE TECNOLOGIA E INFORMÁTICA
Universidade Estadual do Estado de Santa Catarina - CEO

GUIA RÁPIDO DE NAVEGAÇÃO SEGURA NA INTERNET

Orientações gerais para usuários e funcionários da UDESC/CEO sobre a u**tilização de servços, boas práticas e segurança digital.**

Daniele Karoline Carvalho Rosa

O que é Segurança Digital?

Segurança Digital (ou Cibersegurança) é o **conjunto de práticas e ferramentas** que usamos para **proteger nossas informações, dispositivos** (celulares e computadores) e a nossa identidade na internet.

Por que ela é importante?

Segurança Digital não é sobre tecnologia, é sobre comportamento. É o cuidado que você tem com a sua chave de casa, aplicado aos seus cliques na internet.

- **Proteção Financeira:** Evita que criminosos acessem contas bancárias ou façam empréstimos no seu nome.
- **Privacidade:** Impede que fotos, conversas particulares e documentos pessoais vazem.
- **Tranquilidade Profissional:** Evita que o computador de trabalho pare de funcionar por causa de vírus, impedindo que as tarefas do dia a dia se acumulem.

Quais são as ameaças mais comuns?

O "Comprovante" Perigoso

Este é um dos ataques mais eficazes. Você recebe um e-mail com um suposto comprovante de pagamento, nota fiscal ou boleto.

A Armadilha: O arquivo não é um PDF ou imagem, mas sim um arquivo executável (termina em .exe, .scr ou .zip).

O que acontece: Ao clicar para "abrir o comprovante", você instala um programa que dá ao criminoso controle total sobre o seu computador e seus acessos.

Confira este vídeo

E-mail Clonado

Você recebe um e-mail que parece vir de um colega, de um professor ou até de uma instância superior.

- **A Tática:** O criminoso "mascara" o remetente para ganhar sua confiança e pedir que você faça um pagamento urgente ou clique em um link suspeito.
- **Dica de Ouro:** Se o pedido for estranho ou urgente demais, confirme com a pessoa por outro canal (telefone ou presencialmente).

Pop-ups: O Invasor de Telas

Enquanto você navega, janelas saltitantes aparecem dizendo: "Seu Windows está infectado!" ou "Atualize seu navegador agora!".

- **A Verdade:** Quase sempre esses avisos são falsos e servem para te induzir a baixar um vírus ou fornecer dados pessoais.
- **Como agir:** Nunca clique nos botões dessas janelas. Feche a aba do navegador ou use o Alt + F4.

Phishing: Não morda a isca!

O **Phishing** é um método onde **criminosos** enviam mensagens falsas para "pescar" suas senhas ou dados bancários. Eles fingem ser pessoas ou instituições em quem você confia.

Como identificar um e-mail de Phishing?

- **Senso de Urgência:** Mensagens que dizem "Sua conta será bloqueada hoje" ou "Multa pendente: pague agora".
- **Erros de Escrita:** Fique atento a erros de português, falta de acentos ou saudações genéricas como "Prezado cliente" em vez do seu nome.
- **O Link Falso:** Antes de clicar, passe o mouse sobre o link (sem clicar!). O endereço que aparece no rodapé do navegador deve ser exatamente o da instituição oficial. Se o link for www.uudesc.br em vez de www.udesc.br, é golpe.
- **Remetente Estranho:** Verifique se o e-mail do remetente realmente condiz com a empresa. Muitas vezes o nome aparece certo, mas o endereço de e-mail é algo como suporte@gmail.com.

Confira este vídeo

O que fazer se acontecer? (Plano de Contingência)

Cenário 1 (exemplo): Caiu no Comprovante Perigoso dentro setor.

Passo 1: Desconecte o computador da rede/Wi-Fi.

Passo 2: Troque senhas de outros serviços (se usava a mesma).

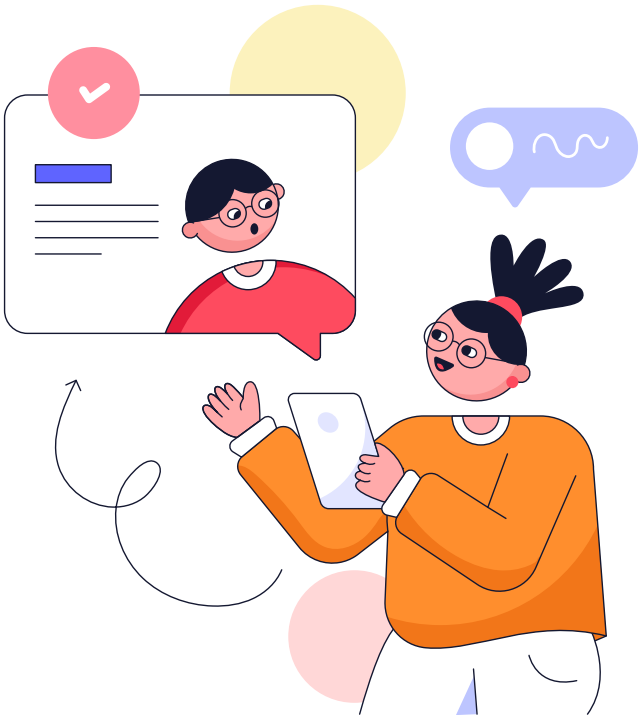
Passo 3: Comunique o setor de TI imediatamente

O computador deve ser desligado?

Se for o golpe do comprovante (.exe): SIM, desligue o computador.

Muitos desses vírus começam a criptografar (trancar) seus arquivos ou roubar senhas assim que são abertos. Desligar força a interrupção do processo malicioso.

Se for apenas um site falso (phishing): Não precisa desligar o PC, mas feche o navegador imediatamente.



Cenário 2 (exemplo): E se for no meu celular ou computador pessoal?

Quando o problema ocorre em um dispositivo que é seu, o risco é dobrado: seus dados bancários e suas credenciais de trabalho estão em perigo.

Se for no Celular (Smartphone)

- **Desconecte o Wi-Fi e os Dados Móveis:** Ative o Modo Avião para impedir que aplicativos maliciosos enviem informações.
- **Revogue Acessos:** Acesse suas contas de outro dispositivo e selecione "Sair de todos os dispositivos" para deslogar golpistas.
- **WhatsApp:** Se perdeu o acesso, reinstale o app e entre novamente. Para desativar a conta, envie um e-mail para support@whatsapp.com com o assunto "Perdido/Roubado".
- **Alerte seus contatos:** Informe em outra rede social ou peça a alguém para avisar nos grupos que seu número foi comprometido.

Se for no Computador Pessoal (Notebook/Desktop)

- **Isole o equipamento:** Desconecte o cabo de rede ou desligue o roteador.
- **Troca de senhas:** Use um dispositivo seguro para alterar senhas do e-mail e banco.
- **Verifique extensões do navegador:** Remova extensões não instaladas por você.
- **Formatação:** Se executou um arquivo suspeito, formate o PC ou use um antivírus confiável.

Mesmo sendo um dispositivo pessoal, se você o utiliza para trabalhar, a TI da Universidade precisa ser informada. Podemos ajudar a monitorar se houve tentativas de acesso ao sistema acadêmico usando o seu usuário logo após o golpe.

Dicas de Segurança e Boas Práticas

Desconfie SEMPRE!

Desconfie de e-mails, SMS ou mensagens de redes sociais com ofertas imperdíveis, pedidos urgentes de dados ou links estranhos, mesmo que pareçam vir de conhecidos.

Autenticação em Duas Etapas (2FA)

Ative a 2FA em todos os serviços essenciais (e-mail, redes sociais, bancos) para uma camada extra de proteção, garantindo que, mesmo com a senha vazada, o acesso seja difícil.

 Como usar a verificação em duas etapas para sua conta Microsoft

Atualizações

Mantenha o sistema operacional, navegador e aplicativos atualizados para corrigir falhas de segurança conhecidas.

Crie Senhas "Fortes e Longas"

Em vez de *senha123*, use algo como *EuAmoCafeComPao2026*!. É mais fácil de lembrar e muito mais difícil de um computador hackear.

Regra dos 5 segundos

Antes de clicar em qualquer link ou baixar um anexo, pare por 5 segundos e pergunte: "Eu estava esperando por isso?", "Eu conheço quem enviou?", "O tom da mensagem é estranho?"

UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA

A segurança da nossa universidade começa com o seu cuidado. Proteger seus dados é proteger a todos nós!

SETOR DE INFORMÁTICA

(49) 2049-9534 | cinf.ceo@udesc.br