

SEC TEAM



SEGURANÇA NA INTERNET

SEGURANÇA NA INTERNET



SENAI

QUEM SOMOS NOS

TURMA DESENVOLVIMENTO DE SISTEMAS



**MATHEUS
VIEIRA**

Desenvolvedor Back-End, Intermediario em Robotica, IoT.

Nick:
ShiroiCrypto



**DAVI
MORENO**

Desenvolvedor Full-Stack, Montagem e Manutenção de Computadores, Redes de Computadores

Nick:
Retro0



**GABRIEL
OLIVEIRA**

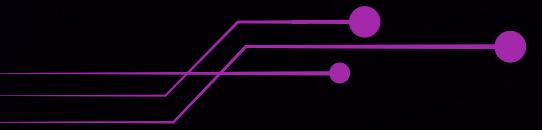
Desenvolvedor Front-End, Modelador de Dados

Nick:
Chilling



**JULIANO
SILVA**

Instrutor de Desenvolvimento de Sistemas, Full-Stack



O QUE É SEGURANÇA NA INTERNET?



É o conjunto de defesas e hábitos que você usa para proteger sua "vida digital". Da mesma forma que você tranca a porta da sua casa, você precisa trancar suas informações no mundo online.

ONDE A SEGURANÇA SE APLICA?

Ela deve estar presente em todos os lugares onde você se conecta:

- Consoles e PCs: Protegendo seu setup.
- Celulares: Onde estão suas fotos e contatos.
- Plataformas de Jogos: Como Roblox, Free Fire e Minecraft.
- Redes Sociais: No Instagram, TikTok e WhatsApp.



NEM TODO MUNDO É QUEM DIZ SER. UM DESCUIDO PODE CAUSAR:

PERDA DE ACESSO AO SEU PERFIL OU CANAL:

A perda de acesso ao YouTube pode ocorrer por senha esquecida, invasão ou suspensão do canal. É possível tentar a recuperação pela Conta Google, verificar e-mails de segurança ou enviar recurso pelo YouTube Studio em caso de suspensão.

USO DA SUA IMAGEM DE FORMA ERRADA:

Uso indevido de imagem é ilegal e gera indenização, conforme o Código Civil e a Constituição Federal. A vítima pode pedir remoção e ação na Justiça em até 3 anos.

PROBLEMAS REAIS QUE AFETAM SUA SAÚDE MENTAL:

Ansiedade, depressão e estresse podem prejudicar a saúde mental; sintomas persistentes indicam necessidade de ajuda profissional.

POR QUE ISSO É IMPORTANTE?

A internet é onipresente, mas exige cautela, pois nem todos são quem dizem ser. Um descuido pode resultar na perda de perfis/canais, uso indevido de imagem e sérios impactos na saúde mental. A exposição excessiva pode levar a riscos reais, sendo essencial proteger a privacidade e os dados pessoais.





CASO FELCA



VISÃO 01

Implementar a restrição de chat como uma camada técnica de defesa, impedindo que vetores de ataque humanos (aliciadores) estabeleçam contato direto com o público vulnerável.

VISÃO 02

Promover o uso de servidores controlados e amizades verificadas, garantindo que o ambiente de jogo não se torne uma porta de entrada para plataformas de comunicação não monitoradas.

DICAS

Chat Off é Proteção On: A proibição do chat não é censura, é uma barreira contra engenharia social e pedidos de dados pessoais.

Mantenha-se na Plataforma: Nunca migre conversas de jogos para WhatsApp ou Discord com pessoas que você conheceu online.



SEGURANÇA NOS JOGOS: ROBLOX



O mundo dos games é incrível, mas para que a diversão não vire dor de cabeça, é preciso conhecer os "bosses" da vida real: os golpistas e os perigos ocultos nos mapas.

1. Cuidado com "Mapas Suspeitos"

Evite "condomínios" ou salas que tentam burlar as regras do jogo. Se o ambiente parecer estranho ou as conversas ficarem inadequadas, saia e denuncie na hora. Não espere o perigo acontecer.

2. O Golpe do "Grátis"

Robux grátis, skins exclusivas ou hacks não existem. * Sites que pedem sua senha para dar prêmios são Phishing (roubo de conta). Links de "vantagens" podem conter vírus que infectam seu celular ou PC.

3. A Regra de Ouro do Chat

Nunca saia do jogo para falar com estranhos. Golpistas tentam te levar para o Discord ou WhatsApp porque lá o Roblox não consegue te proteger. Mantenha suas conversas apenas dentro da plataforma oficial.

Dica Final: Use a Verificação em Duas Etapas e nunca compartilhe sua senha, nem com seu melhor amigo "virtual".



SENHAS SEGURAS

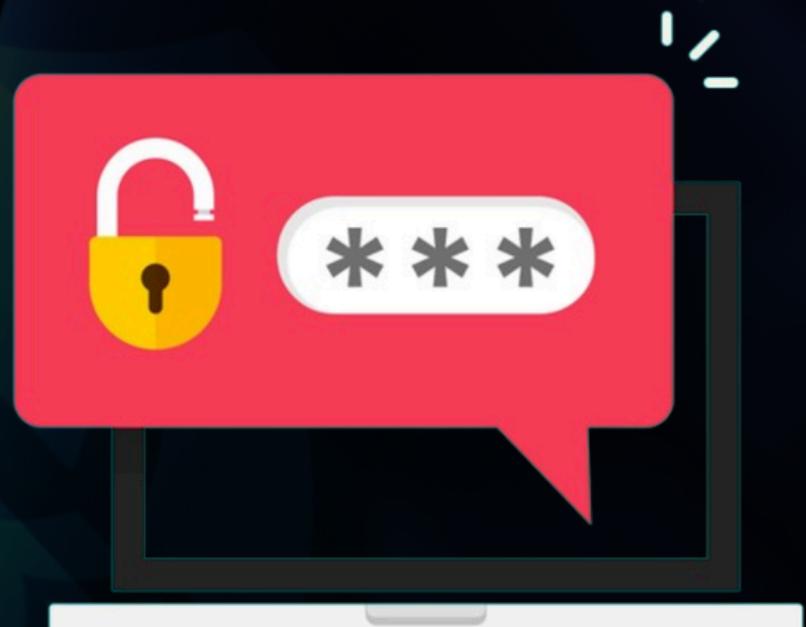
COMO CRIAR UMA "TRANCA" FORTE

Criar senhas fortes é essencial, pois senhas fáceis facilitam ataques de hackers.

O QUE NÃO USAR

Evite senhas óbvias ou fáceis de descobrir, como:

- 123456
- DATA DE NASCIMENTO
- NOME DO PET, FILHOS OU FAMILIARES
- SEU PRÓPRIO NOME OU USUÁRIO
- SEQUÊNCIAS SIMPLES DO TECLADO



O QUE USAR

Uma senha forte deve ter:

- MISTURA DE LETRAS MAIÚSCULAS E MINÚSCULAS
- NÚMEROS SÍMBOLOS (@, #, !, %, &)
- PELO MENOS 8 A 12 CARACTERES (QUANTO MAIOR, MELHOR)

REDES SOCIAIS



CUIDADOS NO INSTAGRAM E TIKTOK

Redes sociais são divertidas, mas podem trazer riscos se você compartilhar informações pessoais demais. É importante proteger sua privacidade e pensar antes de postar.

PRIVACIDADE

- VERIFIQUE SE SEU PERFIL É PÚBLICO OU PRIVADO.
- PERFIS ABERTOS PERMITEM QUE QUALQUER PESSOA VEJA SUAS POSTAGENS.

DICA PRÁTICA

Pergunta para a turma:

"Eu postaria essa foto em um outdoor no centro de Betim?"

Se a resposta for não, melhor não compartilhar online

O QUE NÃO DIVULGAR

- ENDEREÇO DA SUA CASA
- FOTOS COM UNIFORME DA ESCOLA (PODE FACILITAR RASTREAMENTO)
- ROTINA EXATA OU LOCALIZAÇÃO ATUAL

LINKS E MENSAGENS SUSPEITAS



CUIDADO COM O CLIQUE!

Golpes online podem parecer reais, mas seguem padrões comuns. Fique atento e proteja suas contas.

SINAIS DE ALERTA

- MENSAGEM DIZENDO QUE VOCÊ GANHOU UM PRÊMIO QUE NÃO PARTICIPOU.
- TENTATIVA DE CRIAR URGÊNCIA ("SUA CONTA SERÁ EXCLUÍDA EM 2 HORAS!").
- SOLICITAÇÃO PARA DIGITAR SENHA EM SITE ESTRANHO OU DESCONHECIDO.

REGRAS

Na dúvida, não clique. Pergunte a um adulto ou alguém que entenda de segurança online.





CYBERBULLYING: RESPEITO É SEGURANÇA

O respeito na rede é o que nos protege de conflitos e abusos. Cyberbullying não é brincadeira; o ato de ofender, humilhar ou espalhar boatos sobre alguém no mundo digital.



O que fazer se você sofrer ou presenciar:

- Não responda: O agressor busca atenção e reação. Ignorar é a sua primeira defesa.
- Print de tudo: Tire fotos da tela (provas). Elas são fundamentais se for necessário tomar uma medida séria.
- Bloqueie: Não dê uma segunda chance ao desrespeito. Corte o contato imediatamente nas configurações.
- Fale com alguém: Não guarde para você. Procure seus pais, fale com o Juliano ou peça ajuda na coordenação do SESI.

VERIFICAÇÃO DE 2 FATORES (2FA)



VISÃO 01

- Implementar a Verificação em Duas Etapas (2FA) em todas as contas possíveis (Redes Sociais, E-mail e Games).
- Garantir que, mesmo com a descoberta da senha, o invasor seja bloqueado pela camada extra de segurança.

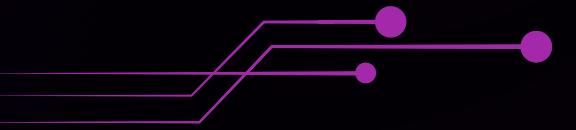
VISÃO 02

- Manter aplicativos e o sistema operacional do celular/PC sempre atualizados para corrigir brechas de segurança.
- Utilizar apenas lojas oficiais (Play Store/App Store) para evitar a instalação de "cavalos de Troia".

DICAS

- Pense antes de postar: Avalie se aquela informação ou imagem pode ser usada contra você no futuro.
- Peça ajuda: Se algo parecer estranho ou se você se sentir desconfortável, procure imediatamente um adulto ou a escola.

SEC TEAM



OBRIGADO

A MELHOR TURMA DO SENAI AGRADECE, ACESSA AI

SENAI