Estratégias e atividades

* O Google não é apenas um mecanismo de busca, mas um ecossistema de serviços digitais. Nesta apostila, vamos explorar as principais funcionalidades do Google e dicas essenciais para sua segurança online.
* Passo 1: Acesse [www.google.com](http://www.google.com/) e clique em "Fazer login" no canto superior direito da tela;



* Passo 2: Clique em "Criar conta". Você terá a opção de criar uma conta para você mesmo ou para gerenciar uma empresa;
* Passo 3: Preencha as informações solicitadas: primeiro nome, sobrenome, nome de usuário (que será seu e-mail) e senha;
* Dicas para Senhas Fortes:
* Uma senha forte é sua primeira linha de defesa contra acessos não autorizados;
* Use pelo menos oito caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos;
* Evite informações pessoais óbvias, como seu nome ou data de nascimento;
* Use senhas diferentes para diferentes contas online;
* Considere o uso de gerenciadores de senhas para ajudar a criar e armazenar senhas seguras.
* Passo 4: Confirme a senha escolhida e siga as próximas etapas, que envolverão verificação de número de telefone e recuperação de e-mail;
* Dica: Use um número de telefone e e-mail de recuperação para aumentar a segurança da sua conta.
* A segurança da senha é crucial para proteger sua conta. Lembre-se de:
* Não compartilhar senhas com ninguém;
* Ativar a autenticação de dois fatores sempre que possível para um nível adicional de segurança;
* **Professor:** Veja este vídeo para melhorar o entendimento <https://www.youtube.com/watch?v=y-PPErxSISo>
* Como exercício para esse módulo você deverá criar uma senha forte e que consiga lembrar: passwordmeter.com.
* Não compartilhe informações pessoais, como número de telefone, endereço ou informações bancárias em sites não confiáveis.
* Esteja ciente de golpes online, phishing e spam que podem tentar enganá-lo para revelar informações sensíveis.
* Phishing é uma técnica que usa e-mails ou sites falsos para obter dados pessoais. Sempre verifique o endereço do site e nunca clique em links suspeitos em e-mails.
* Use um software antivírus atualizado e mantenha seu sistema operacional e programas sempre atualizados para proteger seu computador contra ameaças online.
* E como se defender?
* 1 - Instalar o antivirus;
* 2 - Verificar os arquivos que você recebe;
* 3 - Crie um disco de recuperação (Um HD externo);
* 4 - Tome cuidado com LINKS;
* 5 - Mensagem de conhecido nem sempre é confiável (Pode ter sido falsificado ou invadido por alguém);
* Certificado SSL: Verifique se o site começa com "https". O "s" indica que a conexão é segura.



* Conteúdo: Sites com muitos erros gramaticais ou de design podem ser suspeitos.
* Reputação: Use ferramentas online, como o Safe Browsing do Google, para verificar a reputação de um site.
* Agora solicite aos alunos que tentem, de forma independente, realizar o download do: “Tlauncher” .
* Passo 1: Abra seu navegador de internet (por exemplo, Google Chrome, Mozilla Firefox, Microsoft Edge, etc.);
* Passo 2: Navegue até o site de onde deseja baixar o arquivo;
* Passo 3: Localize o link ou botão que indica o download do arquivo desejado. Geralmente, isso será acompanhado por um ícone de seta apontando para baixo ou uma etiqueta "Download";
* Passo 4: Clique no link de download. O arquivo começará a ser baixado automaticamente para a pasta de downloads padrão do seu computador;
* Antes de fazer o download de qualquer arquivo da internet, verifique a fonte e a confiabilidade do site.
* Evite fazer o download de arquivos de fontes desconhecidas ou suspeitas, pois isso pode representar um risco de segurança.