PROTEÇÃO VIRTUAL
Se você buscar se proteger virtualmente, seria bom dar uma olhada nesses tópicos que serão descritos abaixo
1-Senha forte
2-Atenção nas fontes
3-Não salvar dados nos sites
4-Procurar por alternativas de código aberto
5-Prestar atenção nos formatos dos arquivos que você baixa

COMO SE PROTEGER
Usando de base os tópicos listados anteriormente, vamos descrever cada um deles.

1- Hoje em dia criar uma senha minimamente forte está ficando difícil, porém em uma entrevista Edward Snowden disse como podemos dificultar o acesso de invasores dando dicas de como criar uma senha forte.

Snowden diz que podemos usar frases divertidas e longas, um exemplo que o próprio deu seria
"margartthatcheris110%SEXY"

Essa senha além de ser longa possui números, letras maiúsculas e minúsculas, nomes famosos, adjetivos e caractéres especiais.

2- Se você procurar por algo simples como "Download Skype", verá que aparecerão milhares de páginas, um deles é a que você precisa, porém existem milhares que são falsas e muitas delas podem conter algo malicioso. Portanto sempre busque pelo nome da empresa que desenvolve o software que você precisa, ou então use sites que você já utilizou no passado e não te causaram dor de cabeça.

3- Muitas vezes nós acabamos salvando nossos dados em vários sites para facilitar o acesso, porém pensando no outro lado isso facilita a utilização de seus dados sem permissão, alguém mal-intencionado pode utilizar desde o seu nome até o cartão.

4- Buscar alternativas de código aberto são uma boa pedida, pois a grande maioria além de ser gratuito possui seu código revisado por programadores. Desse modo você está baixando algo confiável.

PRINCIPAIS ATAQUES
Malware é um termo usado para descrever um software mal-intencionado, incluindo spyware, ransomware, vírus e worms. O malware viola uma rede por meio de uma vulnerabilidade, geralmente quando um usuário clica em um link ou anexo de e-mail perigoso e, em seguida, instala o software de risco. Uma vez dentro do sistema, o malware pode fazer o seguinte:

- Bloquear acesso aos componentes principais da rede (ransomware)
- Instalar o malware ou software nocivo adicional
- Obter informações secretamente ao transmitir dados do disco rígido (spyware)
- Prejudicar determinados componentes e tornar o sistema inoperante

Phishing é a prática de enviar comunicações fraudulentas que parecem vir de uma fonte confiável, geralmente por e-mail. O objetivo é roubar dados confidenciais, como informações do cartão de crédito e de logon, ou instalar malware na máquina da vítima. Phishing é uma ameaça virtual que tem se tornado cada vez mais comum.

Ataques man-in-the-middle (MitM), também conhecidos como ataques de espionagem, ocorrem quando os invasores se inserem em uma transação entre duas partes. Quando os invasores interrompem o tráfego, eles podem filtrar e roubar dados.
Dois pontos comuns de entrada para ataques MitM:
1. Em Wi-Fi público não seguro, os invasores podem se inserir entre o dispositivo de um visitante e a rede. Sem saber, o visitante transmite todas as informações por meio do invasor.
2. Uma vez que o malware viola um dispositivo, o invasor pode instalar o software para processar todas as informações da vítima.

Um ataque de negação de serviço (DDOS) inunda sistemas, servidores ou redes com tráfego para esgotar os recursos e a largura de banda. Como resultado, o sistema é incapaz de concluir solicitações legítimas. Além disso, os invasores podem usar vários dispositivos comprometidos para lançar esse ataque.

Uma inserção de **Structured Query Language (SQL**) ocorre quando um invasor insere um código mal-intencionado em um servidor que usa SQL e força o servidor a revelar informações que ele não revelaria normalmente. Um invasor poderia fazer uma inserção de SQL apenas ao inserir um código mal-intencionado na caixa de pesquisa de um site.

Uma **exploração de dia zero** é lançada depois que uma vulnerabilidade de rede é anunciada, mas antes que uma correção ou solução seja implementada. Os invasores têm como alvo a vulnerabilidade revelada durante essa janela de tempo. A detecção de ameaça à vulnerabilidade de dia zero requer atenção constante.