Microsoft

Pense antes de clicar!

Os hackers disfarçam links de phishing e anúncios fraudulentos como fontes confiáveis para te induzir a clicar neles.

Os hackers usam links maliciosos para encontrar um caminho para seus dispositivos, como o seu...

- Tablet
- Telefone
- Computador

Quando eles entram, eles podem...

- Espionar você
- Acessar sua câmera
- Bloquear o dispositivo
- Roubar suas informações
- ...e muito mais

Links maliciosos podem estar em...

- Websites
- Buscadores
- Mensagens de texto
- Emails
- Postagens de mídia social
- Mensagens diretas (DM)

Proteja-se com cuidados cibernéticos!

Procure essas bandeiras vermelhas comuns ao phishing

O que é phishing? O ato de usar mensagens falsas ou links perigosos para tentar roubar suas informações!

- #1 Erros ortográficos ou erros no texto da mensagem
- #2 Informações de contato incorretas ou suspeitas
- #3 O link (ou e-mail do remetente) não está indo para onde você espera
- #4 A mensagem transmite ameaça e urgência
- #5 Solicita que você forneça informações privadas
- #6 Ofertas e pechinchas

Nem todos os links desconhecidos são tentativas de phishing... Eles também podem ser anúncios fraudulentos.

Como identificar um anúncio fraudulento?

- Os anúncios fraudulentos podem parecer anúncios reais, portanto, não assuma que eles são legítimos apenas porque têm uma tag "Anúncio" ou "Patrocinado".
- Ele pode ter bandeiras vermelhas semelhantes a uma mensagem de phishing, como solicitar dados pessoais e oferecer recompensas em troca.

Links de phishing são enviados, enquanto os **anúncios fraudulentos** são links perigosos que você encontra.

Se você receber ou abrir um link malicioso, isto é o que você pode fazer:

- Não tente consertar você mesmo!
- Informe um pai, responsável ou professor imediatamente.