DICAS AP2SI PARA UMA

CIBERSEGURA

Introdução

- A **Black Friday** é o primeiro dia de compras da época natalícia. Com origem nos EUA, está definido como o dia seguinte ao Dia de Ação de Graças, ou seja, celebra-se no dia seguinte à quarta quinta-feira do mês de novembro.
- É uma celebração de promoções que, com o suporte da Internet, se expandiu um pouco por todo o mundo.
- No entanto é também uma época explorada pelos criminosos no ciberespaço e, por isso, a AP2SI produziu este folheto com algumas dicas para si.
- Leia e partilhe. Esperamos que seja útil!

BOAS COMPRAS
EM SEGURANÇA

Phishing

- Recebeu um email com uma promoção excelente? Ou talvez um SMS? Apenas precisam de alguns "*dados seus*" ou de "*confirmar o cartão de crédito"* para "*processar uma oferta*"? Solicitam-lhe que aceda a um site e coloque as suas credenciais para as "*validar*"? Tem apenas 1 dia antes da *"oferta expirar*" ou algumas horas antes da "*encomenda ser devolvida*"?

- As perguntas acima ilustram algumas técnicas conhecidas de *phishing.* São tentativas de recolher informação confidencial de uma pessoa, fazendo-se passar por uma entidade que parece confiável e colocando pressão para uma resposta rápida.

- Nunca forneça os seus dados pessoais ou de cartão de crédito sem verificar quem lhe solicita essa informação. Não clique em links enviados por email ou por SMS. No caso de ofertas, valide com a empresa a sua existência através de contactos oficiais.

Websites falsos

- Durante esta época é habitual o surgimento de vários *websites* falsos que tentam fazer-se passar pelos originais.
- Quem está a fazer a compras deve prestar atenção aos endereços que são mencionados em emails, SMSs, anúncios em redes sociais ou até em suportes físicos como jornais e revistas.
- Leia sempre com atenção os endereços de internet. Aquela letra é um “I” (i maiúsculo) ou um “l” (L minúsculo)? É um “O” (o maiúsculo) ou um “0” (numeral zero)?
- Mantenha-se vigilante e verifique sempre os endereços recebidos. Não clique em links enviados por email ou por SMS. Para uma maior segurança, insira os endereços manualmente na barra de endereços.

Apps falsas

- Tenha atenção ao descarregar e instalar *apps* que prometem encontrar os melhores negócios, as melhores ofertas. À semelhança dos *websites* falsos, também nesta altura é possível encontrar aplicações falsas nas várias *stores* de aplicações como o Google Play ou a Apple Store.
- Estas *apps* falsas tentam executar os mesmos ataques descritos anteriormente – capturar credenciais, números de cartão de crédito ou outro tipo de informação pessoal – prometendo excelentes negócios.
- Pare e pense antes de instalar. Visite a loja do vendedor e verifique se existe uma *app* publicada, com o endereço oficial para a *store.* Se uma oferta parece demasiada boa para ser verdade, geralmente não é verdade.

Software Malicioso

- Existem diversos tipos de software malicioso, como vírus ou cavalos-de-Tróia, que se instalam nos sistemas e permitem que outros possam, maliciosamente, aceder a informação ou ver o que está a ser executado no equipamento onde se instalam.

- Mantenha os seus equipamentos atualizados com as atualizações oficiais do sistema operativo e das aplicações. Use um antivírus. Não instale aplicações ou abra documentos que receba por correio eletrónico sem que seja solicitado ou verificado. Não instale *plugins* ou extensões no seu navegador sem verificar a proveniência.

- Pare e pense antes de instalar uma aplicação ou abrir um documento. Utilize o antivírus sempre que possível. Se não está à espera de uma comunicação, as probabilidades que seja um ataque são bastante altas.

Últimos conselhos

- Não existem ferramentas milagrosas para nos protegermos e qualquer um pode ser uma vítima.
- Utilize cartões de crédito virtuais ao fazer compras *online*. Crie um cartão único com o valor que pretende gastar na compra. Desta forma, mesmo que o mesmo seja comprometido apenas irá perder o valor com que criou o cartão.
- Mantenha os seus sistemas atualizados e sempre que possível utilize autenticação multifactor nos *websites* que utiliza. Desta forma acrescenta segurança adicional aos tradicionais *nome de utilizador* e *password*.
- Esteja alerta e pense criticamente antes de realizar qualquer ação como instalar aplicações, fornecer dados pessoais ou partilhar dados de cartão de crédito.

Imagens:
https://pixabay.com

BLACK FRIDAY

VYPRODEJ

REBAJAS

SALDOS

VYPRODEJ

Promoções espectaculares

Hacking

Apps falsas

SALDOS

SALDI

Segurança

Phishing

Cartão de crédito

SOLDEN

Malware

Websites falsos

SALDI

Dados pessoais

Segurança

SOLDEN

Produzido por:

AP2SI

https://ap2si.org

Siga-nos em: