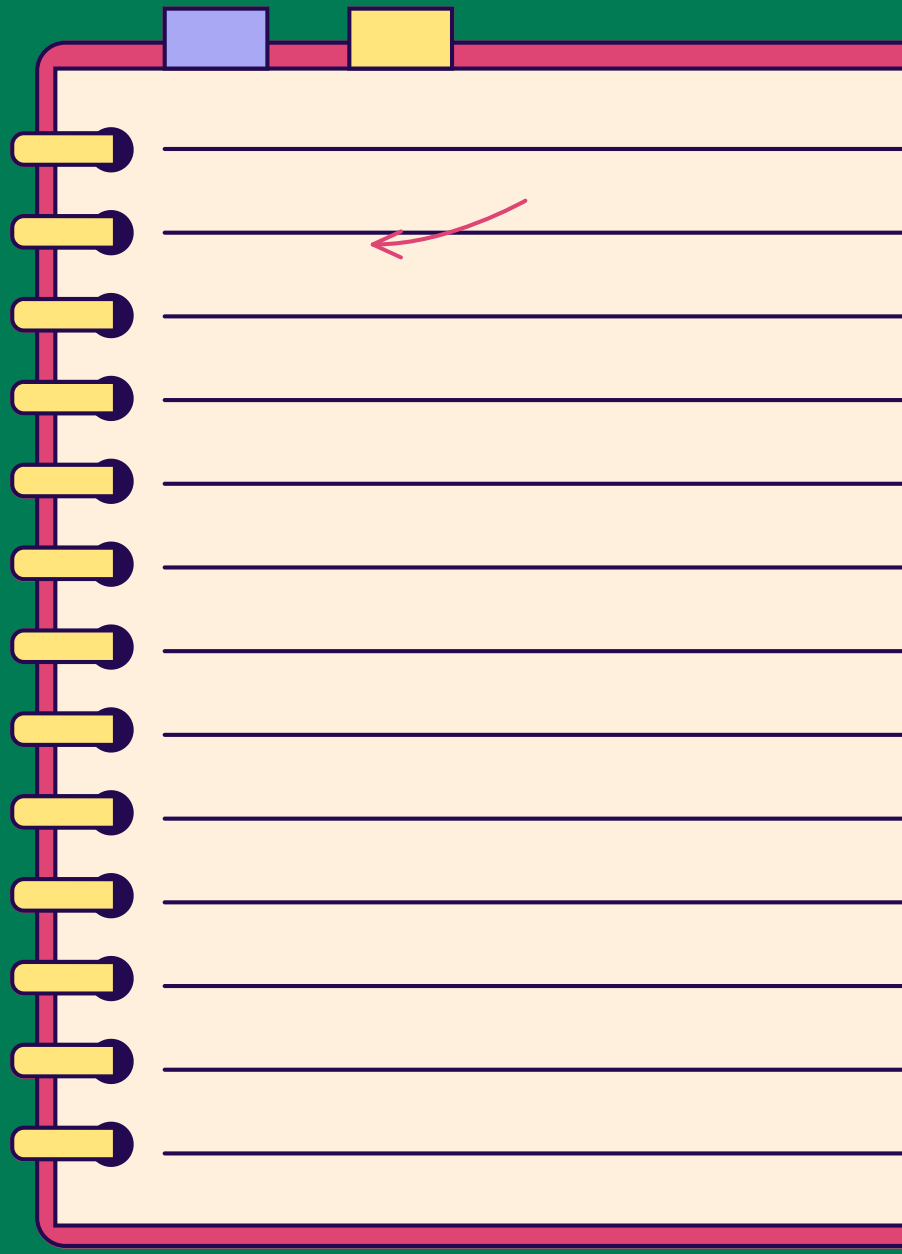
MÓDULO 12 - GOLPES ONLINE

CAPÍTULO 2

COMO PROTEGER-SE CONTRA GOLPES

Skills to Connect



INTRODUÇÃO

Neste capítulo, iremos explorar as melhores práticas para proteger-se contra burlas online. Vai aprender sobre ferramentas de segurança essenciais, como antivírus e firewalls, bem como hábitos simples que pode adotar para garantir a segurança dos seus dispositivos. Também aprenderá a utilizar métodos de proteção adicionais, como a autenticação de dois factores, para manter as suas contas online seguras. No final deste capítulo, saberá como reforçar as suas defesas contra os cibercriminosos.

1 ALGUNS TERMOS PARA ESCLARECER

O QUE É A CIBERSEGURANÇA?

A cibersegurança refere-se a todas as estratégias e tecnologias implementadas para proteger os sistemas informáticos, as redes e os dados contra qualquer forma de ameaça, quer seja maliciosa ou acidental.

- O seu principal objetivo é impedir o acesso não autorizado, o roubo, a corrupção ou a danificação de informações e infraestruturas informáticas. Isto inclui a proteção dos dados pessoais, a segurança das transacções electrónicas e a gestão dos riscos associados a malware, ataques de phishing e violações de segurança.

- Na prática, a cibersegurança baseia-se em medidas técnicas como firewalls, programas antivírus e autenticação por múltiplos factores, mas também inclui aspectos organizacionais como a aprendizagem dos utilizadores e a aplicação de políticas de segurança sólidas para garantir uma gestão adequada dos riscos.

1 ALGUNS TERMOS PARA ESCLARECER

QUAL É A DIFERENÇA ENTRE UM PIRATA E UM HACKER?

A diferença entre “pirata informático” e “hacker” depende geralmente do contexto e da interpretação, pois as definições podem variar.

- **Hacker:** Originalmente, um hacker era alguém que tinha um conhecimento profundo dos sistemas informáticos e de software. Eram apaixonados por tecnologia que gostavam de explorar e compreender sistemas complexos. Os hackers desenvolviam frequentemente competências avançadas de programação e eram capazes de encontrar soluções criativas para problemas técnicos. Dentro desta comunidade, “hacker” tem geralmente uma conotação positiva e está associado à curiosidade e à competência técnica.

- **Pirata informático:** Este termo é frequentemente utilizado para descrever alguém que utiliza competências técnicas para aceder a sistemas informáticos sem autorização e com intenções maliciosas. Os piratas informáticos podem estar envolvidos em actividades como o roubo de informações, o comprometimento de sistemas, a distribuição de malware, entre outras. Ao contrário dos hackers, os piratas informáticos são geralmente vistos de forma negativa e estão associados a actividades ilegais e nocivas.

No entanto, é importante notar que estas definições podem sobrepor-se ou ser interpretadas de formas diferentes, especialmente no contexto em constante mudança da cibersegurança e da cultura tecnológica. Além disso, o termo “hacker” pode ser utilizado de forma mais ampla para descrever uma variedade de indivíduos com conhecimentos técnicos, enquanto “pirata informático” é mais específico das actividades criminosas.

2 PROTEGER-SE CONTRA GOLPES

COMO?

ETAPA 1: PROTEGER OS SEUS DISPOSITIVOS

Antes de mais, é essencial proteger os nossos computadores e dispositivos móveis contra ataques informáticos. Isto inclui a instalação de programas antivírus e firewalls fiáveis, bem como manter todo o software atualizado. Muitos ataques cibernéticos exploram vulnerabilidades em software desatualizado, portanto é essencial manter o sistema atualizado para evitar intrusões.

- **Firewall:** Uma firewall é um sistema de segurança que actua como uma barreira para proteger uma rede informática. Monitoriza as ligações à Internet e decide que dados podem entrar ou sair, de modo a bloquear ameaças ou ataques. Basicamente, impede a passagem de más ligações e protege o computador ou a rede contra perigos.

- **Antivírus:** Um programa antivírus é concebido para detetar e remover vírus e outro software malicioso do seu computador. Protege o seu dispositivo, analisando ficheiros e impedindo que as ameaças infectem o seu sistema. Também desempenha um papel preventivo, impedindo que os vírus causem danos.

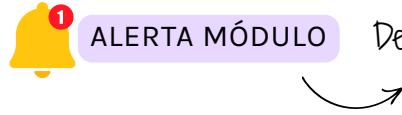
2 PROTEGER-SE CONTRA GOLPES

COMO?

ETAPA 2: PROTEGER AS SUAS CONTAS

A proteção das nossas contas electrónicas é muito importante. Muitas pessoas utilizam senhas simples ou as mesmas senhas para várias contas, o que facilita o roubo por parte dos piratas informáticos.

- É essencial ter **senhas fortes e diferentes para cada conta.**



- Também é aconselhável utilizar a **autenticação de dois factores** sempre que possível:
  - A autenticação de dois factores é um método de segurança adicional para proteger as suas contas online. Em vez de utilizar apenas a sua senha para iniciar sessão, este método pede-lhe duas informações para verificar a sua identidade.
  - O primeiro passo é introduzir a sua senha, como habitualmente. No segundo passo, entra em ação a autenticação de dois factores: recebe um código adicional. Este código pode ser enviado por SMS para o seu telemóvel, por correio eletrónico ou pode ser gerado por uma aplicação como o Google Authenticator.
  - Este código é geralmente válido por um curto período de tempo e é único para cada conexão. Mesmo que alguém consiga roubar a sua senha, será impossível iniciar sessão sem o segundo código. Esta dupla verificação garante que é o único a poder aceder à sua conta, mesmo que outra pessoa conheça a sua senha.

Cada vez mais aplicações e websites exigem autenticação de dois factores, como o Facebook, o Google e a Microsoft.

2 PROTEGER-SE CONTRA GOLPES

COMO?

ETAPA 3: PROTEGER OS SEUS DADOS

É fundamental estarmos conscientes da forma como partilhamos os nossos dados pessoais na Internet e tomar medidas para os proteger. Isto significa limitar as informações que partilhamos nas redes sociais e noutros sites, bem como estar particularmente atento ao preenchimento de formulários online. Os piratas informáticos visam frequentemente dados sensíveis, como números de cartões de crédito, números da segurança social e datas de nascimento, que podem ser utilizados para roubo de identidade ou outras formas de fraude.

Proteger os nossos dados pessoais é, por conseguinte, um passo essencial para evitar as fraudes online. Reduzindo a quantidade de informação que partilhamos e prestando atenção à segurança dos sites que utilizamos, podemos minimizar o risco de sermos vítimas de burlas.

ALERTA MÓDULO

Aprenda como proteger os seus dados com o Módulo 1

PARA LEMBRAR!

Hábitos a adotar para proteger-se de burlas online :

- Aprenda a reconhecer os diferentes tipos de burlas e os sinais a que deve estar atento para não ser enganado
- Proteja os seus dispositivos actualizando-os e instalando firewalls e software antivírus
- Proteja os seus dados e contas utilizando senhas fortes e autenticação de dois factores.