NOVAFCSH
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS
UNIVERSIDADE NOVA DE LISBOA

Dia da Internet Segura - Boas Práticas em Cibersegurança

O Dia da Internet Segura assinala-se na NOVA FCSH, no dia **6 de fevereiro**, com um conjunto de iniciativas destinadas a alertar a comunidade para as possíveis ameaças e medidas de segurança a tomar para as prevenir.

Num tempo em que grande parte da nossa comunicação e lazer se passa dentro de um mundo virtual, a cibersegurança tornou-se uma prioridade para proteger a nossa informação pessoal e profissional. Tanto no mundo físico como no mundo virtual existe um conjunto de boas práticas para a maneira como nos comportamos.

Para garantir uma maior proteção, a NOVA FCSH deixa as seguintes recomendações:

Palavras-passe

As palavras-passe são a primeira linha de defesa contra ameaças cibernéticas. As palavras-passe devem ser fortes, robustas e difíceis de adivinhar. Devemos evitar utilizar o aniversário ou nome como palavras-passe, pois são previsíveis e adivinháveis. Para criar uma palavra-passe forte, é importante seguir as seguintes regras: Mistura aleatória de, pelo menos, 14 a 16 caracteres; Mistura de caracteres numéricos, minúsculos, maiúsculos e especiais.

Uma palavra-passe forte tem o seguinte aspeto: **!C8kpA&CEpfLBt**

A palavra-passe mostrada demora séculos a ser descodificada usando a computação atual. Embora esta seja forte, não é memorizável. E é por isso que há mais um conjunto de práticas a seguir quando lidamos com palavras-passe:

- Não reutilizar a mesma palavra-passe em serviços diferentes;
- Ativar a autenticação de dois fatores (2FA) ou a autenticação multi-fator (MFA), se a
- plataforma dispor;
- Utilizar um gestor de palavras-passe para armazenar, gerar e controlar todas as
- palavras-passe.

É muito importante, hoje em dia, utilizar um gestor de palavras-passe. Com um gestor de palavras-passe, podemos gerar palavras-passe fortes para as nossas contas e guardá-las num único sítio sem precisar de as memorizar. Além disso, um gestor de palavras-passe também permite utilizar autenticações de dois ou multi-fatores, não necessitando de uma aplicação extra.

Phishing

Phishing é um ataque cibernético com o objetivo de nos levar a partilhar informações pessoais, como as nossas palavras-passe ou o número do cartão de débito. Atualmente, os emails e SMS de phishing estão muito sofisticados. É, por vezes, muito difícil perceber que se trata de um ataque de phishing porque estas mensagens já quase não têm erros gramaticais e utilizam imagens manipuladas muito convincentes. Contudo, se seguirmos estes passos será mais fácil detetar que estamos a ser alvo de um ataque de phishing:

- **Desconfiar quando algo é demasiado bom para ser verdade**. Se estão a oferecer algo muito bom, convém desconfiar da verdadeira intenção daquele contacto;
- **Não clicar em links a menos que tenha a certeza da sua origem.** Se o remetente for desconhecido é importante evitar clicar em links. Muitas vezes, é possível pesquisar no motor de busca e encontrar o link que procuramos se for realmente fidedigno;
- **Desconfiar da mensagem quando apela a uma ação imediata.** Quando a mensagem obriga a tomar uma decisão instantânea ou urgente, é porque muito provavelmente é phishing;

- **Analisar atentamente o aspeto gráfico e a linguagem utilizada.** Atualmente, com serviços de tradução grátis e eficientes, as mensagens quase não têm erros gramaticais. Contudo, é algo ainda a ter em conta se acontecer.

Redes Públicas

As redes de Wi-Fi públicas como as encontradas em cafés, restaurantes, transportes públicos ou aeroportos trazem riscos e é preciso ter um cuidado extra quando as utilizamos.

É importante evitar sempre utilizar este tipo de redes pois qualquer pessoa pode controlar e aceder ao tráfego que o nosso dispositivo envia. Devemos antes utilizar os dados móveis do nosso operador. Contudo, se mesmo assim tivermos a necessidade de utilizar estas redes, é importante evitar realizar operações sensíveis, como fazer compras online, iniciar sessão nas contas de email ou em aplicações bancárias.

Segurança do Dispositivo

O nosso dispositivo é a porta de entrada para a nossa vida pessoal. É nele onde guardamos fotos, vídeos, documentos; acedemos ao banco; e comunicamos com familiares e amigos. Por isso, devemos ter cuidado para que ele não caia nas mãos erradas ou fique vulnerável com possíveis falhas no cuidado de saúde do software. No que toca à segurança do dispositivo é importante apostar na prevenção, quer seja um telemóvel ou um computador:

- **Encriptar o dispositivo.** Ao encriptar o dispositivo estamos a criar uma barreira no acesso aos nossos dados caso o caia em mãos alheias. A encriptação dá-nos tempo para apagar o dispositivo remotamente ou recuperá-lo sem a perda ou roubo dos nossos dados;
- **Colocar uma palavra-passe para desbloquear o dispositivo.** É importante definir uma primeira barreira de segurança no dispositivo. Devemos ter cuidado para não revelar a palavra-passe em locais públicos;
- Evitar instalar aplicações de fontes desconhecidas. Instalar aplicações que não se encontram nas lojas oficiais do dispositivo traz riscos para a segurança dos nossos dados e pode permitir a exploração de vulnerabilidades;
- **Configurar o dispositivo para poder ser apagado remotamente.** Caso se dê uma perda ou furto do dispositivo, é importante poder apagá-lo remotamente para que não haja fuga dos nossos dados pessoais;
- **Atualizar aplicações e o sistema operativo.** As atualizações incluem correções de segurança para corrigir vulnerabilidades e proteger o dispositivo de ameaças cibernéticas.

Notícias, imagens e vídeos falsos

As tecnologias de inteligência artificial já são capazes de gerar textos, imagens e vídeos falsos tão perfeitos que não os conseguimos distinguir dos verdadeiros. Com estas "fake news" e "deepfakes", os atacantes, de diversas origens, pretendem levar-nos a mudar as nossas atitudes, comerciais, políticas ou outras. Na Internet devemos ser muito críticos face ao que vemos e só confiar em fontes fidedignas.

Estes são os principais pilares da cibersegurança. Se os seguíssemos à risca, muitas das vulnerabilidades que vemos e ouvimos não existiriam. É connosco que começa e acaba a proteção dos nossos dados e dos nossos dispositivos!

Em caso de dúvida, contacte os Serviços de Informática e Helpdesk da NOVA FCSH através do helpdesk@fcsh.unl.pt

6 de fevereiro de 2024