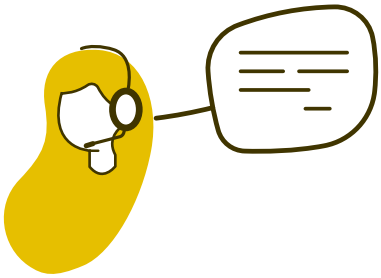
POLITÉCNICO DE LEIRIA

TRABALHAR REMOTAMENTE DE FORMA SEGURA

Melhores Práticas para Teletrabalho

Recomendações do Gabinete de Segurança da Informação do Politécnico de Leiria

GABINETE
SEGURANÇA DA INFORMAÇÃO



MELHORES PRÁTICAS PARA TELETRABALHO

Em tempos de mudanças forçadas por um ambiente de urgência, os ataques de cibersegurança e em especial os de engenharia social, têm estado em evidência nos últimos tempos. Neste tipo de ataques, os atacantes induzem as vítimas em erro de forma a que estas fiquem prejudicadas, o que num período conturbado como o que atravessamos é mais fácil de acontecer.

Como utilizadores de tecnologias e responsabilidades sociais e profissionais, devemos tomar algumas medidas e estar concentrados. Devemos estar atentos para este tipo de ataques, que acontecem não apenas através de mensagens de correio eletrónico, mas também através de outros métodos, como é o caso de chamadas telefónicas, mensagens de texto, redes sociais ou notícias falsas.

Alguns exemplos recentes de ataques associados ao vírus COVID-19

Mensagens de correio eletrónico com informação relativa ao novo vírus no qual atraía os utilizadores a abrir anexos, no entanto, estes seriam programas maliciosos;

Site com uma réplica funcional de um mapa mundial de casos COVID-19 que infetava os computadores utilizados para consultar a informação;

Aplicação COVID-19 Tracker para equipamentos Android que após a sua instalação, “bloqueia o dispositivo e exige um resgate” em bitcoins ao utilizador.

Com o objetivo de garantir a cibersegurança durante o período de isolamento social, seguem algumas recomendações essenciais a ter em conta para quem trabalha remotamente:

- **Não abrir mensagens ou qualquer outro tipo de conteúdos desconhecidos ou suspeitos;**
- **Utilizar palavras-passe robustas;**
- **Garantir que possui o seu sistema atualizado, com antivírus e firewall ativo;**
- **Fazer análises regulares de deteção de vírus e malware;**
- **Não partilhar dispositivos fornecidos pelo Politécnico de Leiria com familiares e amigos;**
- **Fazer cópias regulares de segurança da informação importante do dispositivo;**
- **Não utilizar redes sem fios em espaços públicos;**
- **Utilizar sempre a VPN;**
- **Garantir que a sua rede sem fios de casa tem uma palavra-passe forte;**
- **Nunca confiar em dispositivos de armazenamento USB desconhecidos;**
- **Reportar incidentes ou situações duvidosas.**

NÃO ABRIR MENSAGENS OU QUALQUER OUTRO TIPO DE CONTEÚDOS DESCONHECIDOS OU SUSPEITOS

Todos os dias são enviadas milhares de mensagens com o propósito de comprometer computadores e/ou ganhar dinheiro através de ameaças ao utilizador, fazendo-se passar por entidades fidedignas.

Nos tempos que correm, é aconselhada extrema prudência no acesso, receção e na partilha de conteúdos digitais associados especialmente os que dizem respeito à temática da pandemia COVID-19.

Existem diversos conteúdos fraudulentos que tentam tirar partido desta pandemia com objetivo de ludibriar os utilizadores disseminando códigos maliciosos que bloqueiam computadores ou extrair dados pessoais de contas bancárias ou correio eletrónico.

Em virtude de todos estes casos, deve-se dar prioridade a fontes oficiais e reputáveis de informação.

Seguem alguns cuidados recomendados para sua segurança:

Não abrir mensagens, se o assunto for estranho ou inesperado. Em caso de dúvida contacte os serviços e/ou o remetente da mensagem. Alerta máximo para assuntos relacionados com o COVID-19;

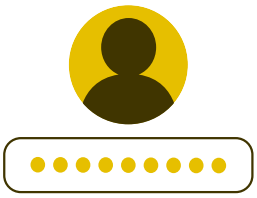
Não abrir ficheiros anexos recebidos de fontes desconhecidas, não solicitadas ou não confiáveis;

Não clicar em hiperligações contidas em mensagens de correio eletrónico, a não ser que sejam de fonte claramente identificada e confiável;

Não enviar palavras-passe, ou outros dados pessoais, em resposta a mensagens de correio eletrónico que solicitam dados, prática conhecida por phishing. Nenhum serviço solicita palavras-chave;

Não enviar ficheiros anexos conhecidos por estarem infetados com vírus ou outros softwares maliciosos;

Se carregar em hiperligações, verifique sempre se o link corresponde à entidade correspondente (Por exemplo, se aparece *www.ipleiria.net* em vez de *www.ipleiria.pt*)



UTILIZAR PALAVRAS-PASSE ROBUSTAS

A utilização de palavras-passe com pouca robustez é um dos principais fatores responsáveis por milhões de violações por todo o mundo. Existem diversos comportamentos a ter em conta para a redução deste risco:

Utilização de Frase-Chave (Passphrases)

Utilização de uma frase sem contexto composta por diversas palavras que seja difícil de descobrir, mas fácil de memorizar. O uso de frases é uma boa forma de construir palavras-passe fortes, para além de ajudar na sua memorização. As palavras-passe construídas desta forma, normalmente são constituídas por letras, números e caracteres especiais que são usados para representar as palavras ou o significado de uma frase. Exemplos:

1. Estratégia com Caracteres

Passo 1
Escolha uma frase - por exemplo:
“Eu vou no autocarro número 14 às sextas-feiras”

Passo 2
Use o primeiro caractere de cada palavra:
E v n a n 14 à s f

Passo 3
Misture com letras maiúsculas e minúsculas:
eVNan14àSf

Passo 4
Adicione caracteres especiais (como! @ # $% ^ & * () _ + | ~ - = \ ` {} []:”; ‘<>?,. /) e números para aumentar a complexidade.

A password final pode ser: E*VNan#14àSf5

2. Estratégia com Frase

Esta estratégia consiste em juntar palavras aleatórias de forma a que formem uma frase longa e sem nexo, tornando a palavra-passe difícil de descobrir. Um exemplo poderá ser:

Utilização de palavras-passe únicas para todas as contas

Não repetir palavras-passe nas diversas contas que possui;

Não utilizar a sua conta profissional para serviços externos

Evitar utilizar a conta @ipleiria.pt para registo em serviços externos como por exemplo Dropbox, Facebook, etc;

Utilizar gestores de palavras-passe

Existem programas especiais para fazer o armazenamento de forma segura de palavras-passe, sendo apenas necessário memorizar a palavra-passe para aceder ao programa. Ex.: KeePass, TK8 Safe, Last Pass.

Todos os utilizadores dos sistemas de informação do Politécnico de Leiria são dotados de nome de utilizador (i.e. username), que é pessoal e intransmissível, e uma palavra-passe confidencial, que os identificará univocamente perante os sistemas de informação do Politécnico de Leiria e, por consequência, os responsabilizarão pelas ações realizadas com as suas contas.

O acesso aos sistemas de informação do Politécnico de Leiria é concedido individualmente. **Cada utilizador é responsável por manter a confidencialidade dos seus dados de acesso aos sistemas**. Em virtude da importância na salvaguarda da segurança, todos devem estar cientes de como construir e escolher palavras-passe fortes e quais as melhores práticas no seu manuseamento.

TODOS OS UTILIZADORES DEVEM ALTERAR A SUA PALAVRA-PASSE SEGUINDO AS RECOMENDAÇÕES

Para alterar a palavra-passe deverá seguir as instruções existentes na intranet do Politécnico de Leiria (https://intranet.ipleiria.pt).

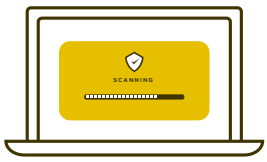
GARANTIR QUE POSSUI O SEU SISTEMA ATUALIZADO, COM ANTIVÍRUS E FIREWALL ATIVO

As atualizações de software desempenham um papel importante na segurança de qualquer dispositivo.

Perante as ameaças que surgem através das mensagens de correio eletrónico e dos sites maliciosos, é determinante que os dispositivos estejam atualizados e protegidos para que possam minimizar a superfície de ataque dos malfeitores.

É essencial que o dispositivo usado para aceder aos recursos do Politécnico de Leiria se encontre atualizado e com as versões mais recentes de software. Verifique se o seu dispositivo está atualizado, se tem o antivírus ativo e atualizado e a firewall ligada. Se o dispositivo for propriedade do Politécnico de Leiria e necessitar apoio contacte os serviços através de suporte.dsi@ipleiria.pt.

Dispositivos que não cumpram os requisitos mínimos de segurança e que, de alguma forma comprometam a segurança do Politécnico de Leiria, poderão ser proibidos de aceder aos recursos disponibilizados pelo Politécnico de Leiria.



FAZER ANÁLISES REGULARES DE DETEÇÃO DE VÍRUS E MALWARE

Os utilizadores acedem constantemente a recursos e documentos importantes da organização através dos seus próprios dispositivos.

Tendo em conta que estes dispositivos estão sujeitos a contrair vírus e *malware* muito facilmente sem que o utilizador perceba, é recomendado que sejam feitas regularmente análises de deteção dos mesmos, através da ferramenta de antivírus instalada nos dispositivos. Esta recomendação inclui também dispositivos móveis.

NÃO PARTILHAR DISPOSITIVOS FORNECIDOS PELO POLITÉCNICO DE LEIRIA COM FAMILIARES E AMIGOS

De forma a garantir a privacidade e segurança dos dados e sistemas do Politécnico de Leiria, os dispositivos fornecidos pelo Politécnico de Leiria devem ser usados exclusivamente por utilizadores autorizados. A instalação de software no dispositivo deverá ser autorizada pelos serviços informáticos do Politécnico de Leiria.

FAZER CÓPIAS DE SEGURANÇA REGULARES DA INFORMAÇÃO IMPORTANTE DO DISPOSITIVO

A execução de um programa malicioso, poderá destruir todos os seus ficheiros ou bloqueá-los em troca de um resgate. Para evitar que isso aconteça, deverá realizar frequentemente cópias de segurança da informação considerada importante e/ou confidencial no seu dispositivo.

As cópias de segurança deverão ser feitas preferencialmente para o OneDrive do Office 365, garantindo assim que as últimas versões encontram salvaguardadas em caso de incidente.

O armazenamento de ficheiros na nuvem garante que os seus ficheiros sejam acessíveis de qualquer lugar e estejam armazenados em segurança.

Adicionalmente os docentes e colaboradores podem também efetuar cópias de segurança via VPN para o seu espaço no Saturno3.ipleiria.pt.

UTILIZAR SEMPRE A VPN

Medida apenas aplicável a docentes ou colaboradores

Ao utilizar a VPN, é criado um “túnel” privado entre o seu computador e a rede do Politécnico de Leiria, permitindo assim o acesso a recursos restritos de forma segura e privada. No entanto, uma VPN não é garantia de segurança absoluta, como tal, mesmo durante a utilização da VPN, deverá ter em conta os princípios básicos de segurança referidos neste documento onde se destaca a atualização de dispositivos, bloqueio de ecrã e utilização de palavras-passe fortes e exclusivas para todas as suas contas.

Para configurar a VPN deverá seguir as instruções existentes na intranet do Politécnico de Leiria (https://intranet.ipleiria.pt).

NÃO UTILIZAR REDES SEM FIOS EM ESPAÇOS PÚBLICOS

Em lugares como aeroportos, cafés, shoppings, restaurantes e hotéis são disponibilizadas redes públicas sem fios. Neste tipo de redes a segurança é descurada ou inexistente por parte dos seus proprietários, privilegiando sim a disponibilização do serviço. A sua utilização acontece sem que os utilizadores avaliem os riscos de se ligarem a redes conhecidas pela distribuição de malware e observáveis por atacantes. A utilização de redes sem fios de espaços públicos deverá ser evitada. Se por alguma razão for necessário utilizar uma rede pública deverá ter os seguintes cuidados:

- Ligar a VPN do Politécnico de Leiria garantindo assim que a comunicação é privada;
- Apenas visitar sites usando HTTPS;
- Fazer o Logout das suas contas depois de as usar.

GARANTIR QUE A SUA REDE SEM FIOS DE CASA TEM UMA PALAVRA-PASSE FORTE

A rede sem fios doméstica não está livre de perigos sendo um alvo apetecível para atacantes. Uma rede desprotegida ou com palavra-passe fraca pode levar à perda de ficheiros, dados pessoais ou profissionais. Para aumentar a sua segurança é importante que faça a mudança da palavra-passe da sua rede sem fios, escolhendo uma palavra-passe forte. Também não deverá partilhar a palavra-passe da sua rede com visitas devendo para este efeito criar uma rede de visitas.

NUNCA CONFIAR EM DISPOSITIVOS DE ARMAZENAMENTO USB DESCONHECIDOS

A maioria das pessoas assume que dispositivos de armazenamento USB como, PENS ou Discos, são dispositivos benignos e confiáveis. Na realidade, estes dispositivos são a porta de entrada de diversos ataques e responsáveis pela distribuição de malware. Qualquer dispositivo desta natureza poderá estar infetado, muitas vezes de forma mascarada através de ficheiros legítimos como músicas ou PDFs. A desconfiança é a palavra de ordem a ter em conta na ligação de dispositivos desconhecidos USB no seu dispositivo.

REPORTAR INCIDENTES OU SITUAÇÕES DUVIDOSAS

Um incidente de segurança é qualquer tentativa, acesso não autorizado, uso, divulgação, modificação ou destruição de informação incluindo ações de hackers e roubo.

Seguem alguns exemplos de incidentes de segurança:

- Violação de sistema e/ou computador;
- Acesso não autorizado a sistemas, software ou dados;
- Alterações não autorizadas a sistemas, software ou dados;
- Perda ou roubo de equipamento que armazena dados institucionais;
- Ataque de negação de serviço;
- Contas de utilizador comprometidas;
- Envio de mensagens de *Phishing.*

É importante que incidentes de segurança reais ou suspeitos sejam reportados o mais rapidamente possível, para que se possa limitar os danos e os custos de recuperação. Como tal deverá proceder da seguinte forma:

- Relate qualquer ação incomum. Se achar que poderá ser um problema não ignore. REPORTE;
- Reporte imediatamente suspeitas de incidentes e violações de segurança;
- Se acha que o seu computador está comprometido ou se alguém acedeu ao mesmo de forma remota, desligue as ligações de rede e peça ajuda.

TODOS OS INCIDENTES DE SEGURANÇA, SUSPEITAS OU SITUAÇÕES DUVIDOSAS DEVERÃO SER REPORTADAS PARA O SERVIÇO DE RESPOSTA A INCIDENTES DO GABINETE DE SEGURANÇA DE INFORMAÇÃO DO POLITÉCNICO DE LEIRIA ATRAVÉS DO ENDEREÇO SUPORTE.GSI@IPLEIRIA.PT.

POLITÉCNICO DE LEIRIA