Módulo de Aprendizagem

Fluxo de informação e comunicação *online*

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do autor: bit schulungscenter
Última data de processamento: 28.10.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Fluxo de informação e comunicação *online*

Introdução

A Internet influenciou massivamente a forma como comunicamos uns com os outros. Para a maioria de nós, a comunicação *online* representa uma parte integrante da nossa vida quotidiana. Todos os dias, inúmeros *emails* são abertos, encaminhados e respondidos. Deste modo, a informação pode ser transmitida de forma rápida, fácil e rentável. Imagine que o programa que utiliza para ver os *emails*, por algum motivo, não funciona corretamente? Não é nada que uma pesquisa rápida na Internet não resolva - facilmente conseguimos encontrar um fórum onde alguém descreve problemas semelhantes ou outros utilizadores partilham dicas úteis com a comunidade *online*. Como se vê, não há dúvidas de que a comunicação *online* oferece muitas vantagens. No entanto, a utilização diária de *emails* e outros meios eletrónicos de comunicação, que muitas vezes tomamos por garantida, tenta as pessoas a tornarem-se descuidadas e, assim, a reconhecerem potenciais riscos demasiado tarde ou não os reconhecerem de todo. Isto sublinha a importância de saber a que se deve realmente prestar atenção quando se utiliza a comunicação *online,* de modo a reduzir o risco de consequências negativas.

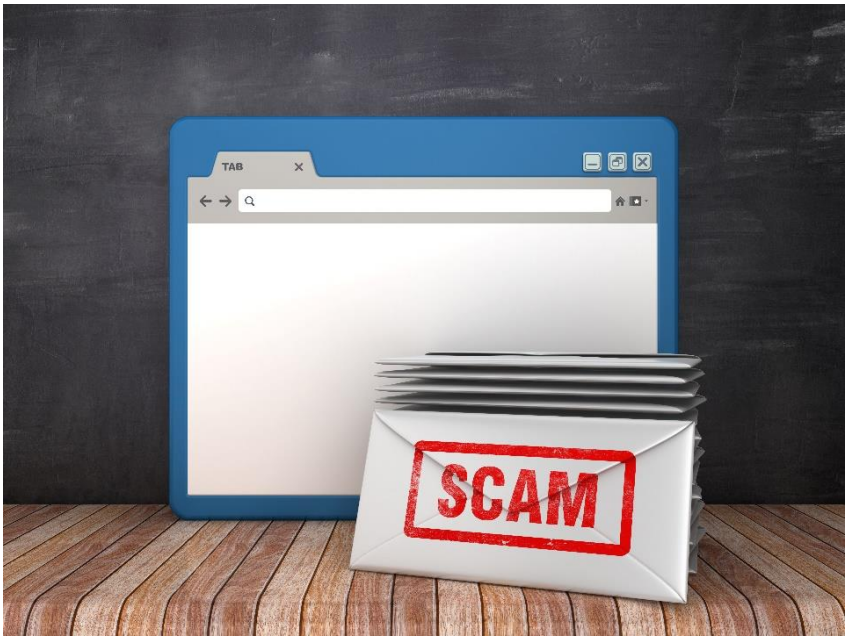
Relevância Prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

A crescente utilização da Internet e de vários instrumentos de comunicação eletrónica - tanto na nossa vida privada como profissional - está a criar ameaças adicionais à segurança dos nossos dados e à nossa privacidade. Por conseguinte, é importante conhecer os riscos atuais em matéria de proteção de dados, a fim de poder reconhecê-los rapidamente e reagir corretamente, se necessário. Em tempos de aumento da cibercriminalidade, o *know-how* adequado sobre possíveis problemas de segurança no decurso da comunicação *online*, bem como o tratamento correto e seguro das mensagens de *email* é uma necessidade para cada utilizador da Internet.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Desenvolver conhecimentos – *Emails* falsos e anexos

O **meio de comunicação *online* mais popular é o *email***; abrir e enviar *emails* já faz parte da rotina diária de quase todos nós. Mas, precisamente devido à grande popularidade da comunicação por correio eletrónico, os ***emails* falsos** são também uma ameaça comum.



Definição
Os ***emails* falsos** são *emails* indesejáveis que induzem as pessoas em erro com informações enganosas, de má-fé ou que conduzem à prática de atos danosos. Por exemplo, os programas maliciosos são frequentemente transferidos para *emails* falsos através de **anexos**.

Assim, é importante prestar atenção às características típicas das mensagens de *email* maliciosos. Antes de abrir anexos, clicar em *links* ou responder a *emails*, **é crucial questionar**:

1. Este *email* promete algo **bom demais para ser verdade**? Isso é um sinal de alerta: Se é bom demais para ser verdade, provavelmente não é real.

Exemplo
Exemplos deste tipo de situações normalmente incluem senhoras muito atraentes que querem conhecer-te, presentes gratuitos ou a notificação de que ganhaste um prémio (apesar de não teres participado em concurso nenhum).

2. O conteúdo do ***email* não bate certo de forma nenhuma com o (suposto) remetente fiável do *email***?

Exemplo
Recebeste um *email* da tua amiga Ana. Ela escreve que está de férias no estrangeiro e que foi vítima de um roubo. Por isso, a Ana pede-te que transfiras imediatamente o dinheiro para uma conta para que ela possa apanhar o último avião de regresso a casa esta semana. Tal conteúdo indica claramente que a conta de correio eletrónico da tua amiga Ana foi pirateada.

3. O *email* contém determinadas **palavras irritantes no assunto**, como "último aviso", "conta bloqueada" ou semelhantes? É solicitado dados de acesso, palavras-passe ou outras **informações confidenciais**?

Importante
Sempre que alguém te incita a apressar ou a revelar informações confidenciais, isso deve fazer soar os sinais de alarme!

4. O **remetente parece estranho** (por exemplo, um *email* em inglês vindo de uma empresa alemã)? A mensagem contém muitos **erros ortográficos ou gramaticais** (provavelmente devido a programas de tradução automática)?

5. O *email* foi automaticamente transferido para a **pasta de *spam***?

Podes estar a pensar agora: “porque é que devo sequer pensar em *emails* de *spam*?”. Muitos fornecedores de correio eletrónico estão constantemente a melhorar a sua monitorização automática e, por conseguinte, normalmente, as mensagens indesejadas acabam automaticamente na chamada pasta *spam*. O problema, contudo, é que também pode acontecer que um *email* esperado seja, ainda que de forma errada, considerado potencialmente indesejado e acabe na pasta de spam.

Exemplo
Um amigo vai dar uma grande festa no seu aniversário. Ele envia os convites por *email* para muitos convidados simultaneamente, introduzindo todos os endereços de *email* em BCC. Infelizmente é possível que o teu convite acabe na pasta do spam, uma vez que muitos endereços em BCC são um sinal típico de correio *spam*.

6. É solicitada a execução de programas com nomes de ficheiros estranhos (por exemplo, composições de nomes de ficheiros conhecidos como "jpg.vbs" ou "gif.exe")?

Se a resposta a uma ou mais destas perguntas for "Sim" ou se uma mensagem *email* parecer suspeita por outras razões, **não se deve abrir o correio** ou os ficheiros e ligações que contém.

Os chamados "***emails* de *phishing***" requerem uma atenção especial.

Definição
O termo ***phishing*** é composto por duas palavras: "***password***" e "pesca (*fishing*, em inglês)". *Phishing* é a tentativa de **obter palavras-passe alheias** com a ajuda de *emails* falsos.

Co-funded by the
Erasmus+ Programme
of the European Union

A maioria de nós já recebeu um ***email*** **estranho** de um seu banco ou de uma loja *online* que conhecemos. Em muitos casos, estes *emails* informam de que infelizmente os dados de utilizador se perderam ou a palavra-passe expirou ou que uma nova identificação é urgentemente necessária devido a uma atualização. Convenientemente, é normalmente enviado diretamente um **link para o *website* da empresa**. Estas páginas *online* são **muito parecidas** com as mensagens legítimas dessas organizações mas são **falsas**. Quando se introduz de boa fé os dados de acesso ao banco ou à loja *online*, os infratores terão acesso aos mesmos e poderão causar sérios danos.

Dicas
As mensagens em que é solicitada a divulgação de dados de utilizador nunca devem ser respondidas dado que as empresas sérias não o requereriam. Se ainda persistirem dúvidas, faz todo o sentido contactar o alegado remetente por telefone!

Além disso, as seguintes medidas podem ajudar a reduzir o risco de comunicação *online* via *email*:

- Ativar a **visualização da extensão do ficheiro** (por exemplo, .docx, .exe). Isto permite identificar melhor os programas maliciosos enviados como anexos de *email*.
- Utilizar definições de segurança apropriadas para impedir a execução de conteúdo ativo em programas de *email*. Por exemplo, pode impedir a **execução de *malware*** indesejado quando uma mensagem é aberta.
- **Guardar primeiro os anexos suspeitos**, para que possam ser verificados com um programa antivírus.

1.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_01_01

Situação: O que significa o termo "*email* falso"?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Os *emails* falsos são *emails* indesejados, que muitas vezes contêm *malware* enviado através de anexos.
- Os *emails* falsos fornecem frequentemente informações falsas ou infundadas.
- Os *emails* falsos podem nem sequer ter sido enviados pelo alegado remetente.

- Os *emails* falsos são mensagens de correio eletrónico sem qualquer conteúdo. Estes *emails* em branco foram enviados intencionalmente ou como uma mensagem acidental.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_01_02

Situação: Ao verificar a caixa de entrada do teu *email*, reparas que tens imensos *emails* novos. Qual dos seguintes casos é mais provável ser falso?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- O *email* promete um enorme prémio.
- É pedido com urgência que alteres os dados de *login* de uma plataforma.
- O *email* não tem assunto.
- O assunto inclui as palavras "aviso final".
- O *email* contém um número percetível de erros ortográficos.
- O *email* foi automaticamente movido para a pasta de *spam*.
- O *email* foi enviado de madrugada.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_01_03

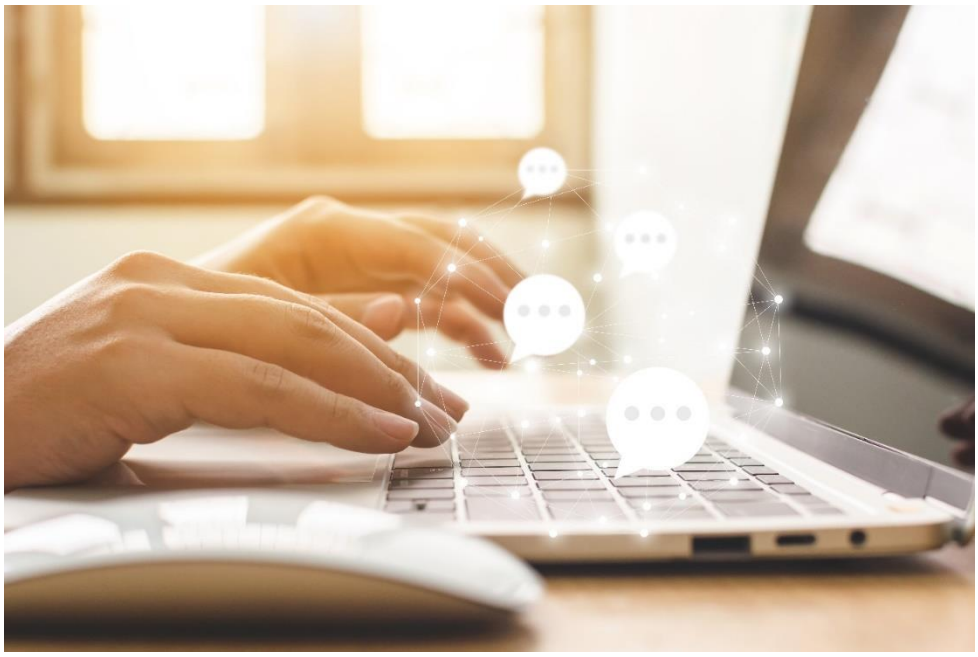
Situação: Quais as medidas que podem ajudar a reduzir o risco de comunicações *online* via *email*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Ativar a visualização da extensão do ficheiro (por exemplo,. docx, .exe).
- Desativar a visualização da extensão do ficheiro.
- Usar definições de segurança apropriadas para impedir a execução de conteúdos ativos em programas de correio eletrónico.
- Verificar anexos suspeitos com um programa antivírus.
- Só divulgar dados de utilizador se se conhecer muito bem as empresas que os estão a solicitar.

2.Desenvolver conhecimentos - Fóruns e salas de *chat*

Os **fóruns** e as **salas de *chat*** são ambos meios de comunicação muito conhecidos e populares para a comunicação e troca de informações *online*, mas diferem na forma como são utilizados.

Co-funded by the
Erasmus+ Programme
of the European Union



Definição
Enquanto os *chatrooms* se direcionam à comunicação com as pessoas **em tempo real**, os fóruns são mais adequados para **discussões em que nem todos os participantes precisam de estar *online* ao mesmo tempo**. Os fóruns normalmente também são mais organizados com discussões divididas em tópicos que tendem a ser moderados por uma terceira pessoa.

Os *chats* e os fóruns permitem a troca de mensagens de texto, mas podem também ser usados para trocar imagens, vídeos, *links* ou ficheiros. Além disso, algumas salas de *chat* também permitem a utilização de microfones ou *webcams* para conversar com outros utilizadores.

A fim de participar ativamente em fóruns e *chat*s, normalmente é necessário um **registo com um endereço de *email* válido**. Isto serve, por exemplo, para evitar publicações de *spam*. Além disso, os moderadores também têm a opção de suspender ou bloquear os utilizadores de fóruns ou *chat*s que se comportem de forma inadequada. No entanto, a utilização destes meios de comunicação pode resultar em vários riscos e ameaças, o que inclui, por exemplo:

- ***Malware* ou *links* para sites de *phishing***: Todos os ficheiros e *links* colocados em fóruns devem, portanto, ser tratados com cautela.
- Deve-se ter em mente que a falsificação ou *hacking* de contas de utilizadores pode induzir em erro, levando outros utilizadores a acreditar em **identidades falsas**.
- A comunicação em fóruns e *chats* é, normalmente, **completamente não encriptada**, pelo que as declarações e informações escritas nestes espaços podem ser lidas por todos os utilizadores. Os *hackers* profissionais são, inclusive, capazes de ler mensagens privadas.

Não queres deixar de usar fóruns e *chats* e queres saber o que podes fazer para evitar riscos de segurança? Deves considerar os seguintes aspetos:

- Não abrir ficheiros recebidos por parte de um destinatário desconhecido/suspeito.
- Nunca transmitir dados pessoais e sensíveis a pessoas que não conheças pessoalmente.
- **Nunca permitir que ninguém aceda ao teu computador**, nem mesmo dentro de uma sessão de *chat*.

Exemplo
Tens um problema informático e estás à procura de conselhos num *chat* de peritos. Um suposto perito quer ajudar-te. É por isso que deves dar-lhe o controlo do computador por controlo remoto.

- **Ler os termos e condições gerais** e **os regulamentos de proteção de dados do serviço de comunicação**, particularmente no que diz respeito ao destino dos dados e informações. São vendidos, armazenados ou encriptados?
- **Bloquear os contactos** se não tiveres a certeza de quem são as pessoas que estão a tentar interagir contigo ou se alguém te estiver a assediar. Deves denunciar insultos, assédio sexual, chantagem ou ameaças à polícia.
- Não esquecer os **direitos de autor**: não enviar fotografias ou outros ficheiros que não tenhas criado, sem a autorização do autor.
- **Ser sempre cauteloso ao namorar com um estranho** que só conheces através de fóruns ou *chats*. Mesmo que tenhas a impressão de que já conheces a pessoa, as informações e declarações fornecidas por essa pessoa podem ser todas falsas ou inventadas.

2.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_01

Situação: O que são salas de *chat* e o que são fóruns? Como é que as ferramentas diferem uma da outra?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- As salas de *chat* são muito adequadas para discussões em que nem todos os participantes têm de estar *online* ao mesmo tempo.
- Os fóruns são mais adequados para falar com os outros em tempo real do que as salas de conversação.
- Podem trocar-se mensagens de texto tanto em salas de *chat* como em fóruns. Muitas vezes, também se podem trocar imagens, vídeos, links, ou ficheiros.
- Os *chatrooms* são mais adequados para comunicar com outras pessoas em tempo real do que os fóruns.
- Embora seja possível conversar anonimamente ou sob um pseudónimo em salas de *chat* é necessário revelar o nome verdadeiro nos fóruns.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_02

Situação: Os fóruns e salas de *chat* são ferramentas muito populares de comunicação *online*. No entanto, qual dos seguintes riscos podem surgir durante o uso destas ferramentas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- A utilização de *software* malicioso através da abertura de ficheiros partilhados em salas de *chat* ou fóruns.
- O redirecionamento para *sites* de *phishing* através do clique em *links* partilhados.
- Custos monetários muito elevados por causa de alguma troca de mensagens em fóruns.
- Alguém tentar enganar outros utilizadores fazendo uso de uma identidade falsa ou inventada.
- A intromissão e leitura por parte de terceiros de mensagens de *chat* enviadas em privado para uma pessoa.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_02_0

Situação: Quais das seguintes medidas podem ajudar a reduzir o risco das comunicações *online* via fóruns e salas de *chat*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Ler os termos e condições gerais do serviço de comunicação.
- Bloquear os contactos que não se conhece.
- Partilhar apenas fotografias ou ficheiros que não tenham sido concebidos pelo próprio.
- Só permitir que alguém aceda ao computador pessoal se tiver uma foto de perfil e um nome de utilizador de confiança.
- Não abrir ficheiros recebidos de forma suspeita.

3. Desenvolver conhecimento - Comunicação em redes sociais

Nas redes sociais, a presunção de anonimato pode levar a um **comportamento imprudente no tratamento de dados e informações**. Como resultado, as redes sociais estão cada vez mais a ser alvo de atividades fraudulentas.

Deve-se sempre **considerar os seguintes aspetos** quando se lida com as redes sociais:

- Nunca publicar e discutir informações pessoais e confidenciais no espaço virtual público. Publicar alegações imprudentes e improváveis pode ter consequências legais graves.
- Cada rede social tem a opção de tornar as informações pessoais acessíveis apenas a certas categorias de grupos de pessoas através de filtros. É prudente verificar estas opções para nunca correres o risco de teres de receber milhares de estranhos na tua festa de aniversário privada.
- Gostas de ter o maior número possível de amigos nas redes sociais? Tem o cuidado de não esquecer o bom e velho ditado: "Mostra-me com quem andas e eu digo-te quem és". **Aceitar amigos de forma crítica pode ter um efeito negativo sobre ti próprio** - como por exemplo, se estiveres à procura de um emprego. Muitos empregadores informam-se sobre as atividades dos candidatos nas redes sociais e usam esta informação para tomar decisões de seleção no processo de candidatura.
- Verifica sempre as configurações das redes sociais para garantires a proteção da tua privacidade.
- É importante estar ciente de que, especialmente nas redes sociais, existe o **risco de ser enganado**. Os piratas informáticos enganam e manipulam deliberadamente as suas vítimas, fornecendo-lhes informações enganosas ou potencialmente perigosas.

Importante
Quando detetamos uma má utilização ou má conduta nas redes sociais, podemos e devemos denunciá-la ao prestador de serviços e às autoridades ou organizações apropriadas.

3.Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_03_01

Situação: O que se deve fazer ao utilizar as redes sociais para evitar possíveis consequências negativas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Aceitar o maior número possível de pedidos de amizade para parecer o mais popular possível para os outros.
- Verificar sempre as definições das redes sociais para proteção da privacidade.
- Não acreditar em toda a informação que aparece nas redes sociais.
- Se não gostas de alguém e gostarias de publicar comentários muito negativos sobre essa pessoa, tem cuidado para não usares o teu nome verdadeiro, especialmente se usares uma linguagem mais dura. Desta forma, poderás permanecer anónimo e não terás de temer consequências.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_03_02

Situação: Estás a usar a tua conta nas redes sociais. Enquanto estas a ver as tuas redes sociais ficas em choque, descobres que alguém publicou um vídeo que mostra um grupo de adolescentes a intimidar e a abusar de uma rapariga tanto física como psicologicamente. Como deves reagir?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Deves denunciar o vídeo ao fornecedor do serviço (por exemplo, Facebook)

- Infelizmente, não há nada que se possa fazer. Talvez o vídeo não seja sequer real. Para evitares ser ameaçado, deves ignorar o mesmo.
- Deves denunciar o vídeo à polícia.
- Não conheces a vítima nem o agressor, pelo que não irás saber dar um nome concreto a ninguém e, portanto, não vale a pena interferires.

Fontes

wko.at: https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/*chat*/

*online*sicherheit.gv: https://www.*online*sicherheit.gv.at/gefahren_im_netz/soziale_medien/gefahren/250080.html

securitymetrics.com: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-*email*

ftc.gov: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

smallbusiness.com: https://smallbusiness.chron.com/differences-between-*chat*-rooms-forums-71296.html

socialnomics.net: https://socialnomics.net/2017/11/08/*chat*ting-*online*-risks-the-tips-to-stay-safe/

getsafe*online*.org: https://www.getsafe*online*.org/social-networking/*chat*rooms/

cybersecurity.edu: https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/social-media

Para relembrar

Resumo

A forma mais popular de comunicação *online* é o ***email***, razão pela qual os ***emails* falsos** também são, infelizmente, bastante comuns. Os *emails* falsos são *emails* indesejados com informações intencionalmente falsas ou enganosas. Por exemplo, o ***malware*** esconde-se frequentemente nos **anexos** de mensagens falsas que são enviadas através de correio eletrónico.

Para não cair no erro de abrir/interagir com estas mensagens de correio eletrónico falsas, **é importante que nos mantenhamos alerta**. Por exemplo, as mensagens de *email* que prometem uma grande recompensa ou que pedem para revelar informações confidenciais devem ser sempre tratadas com muita cautela. O mesmo se aplica às mensagens de correio eletrónico com assuntos desagradáveis como "A sua conta bancária foi bloqueada" ou com um número invulgarmente elevado de erros gramaticais e/ou ortográficos.
Deve ser tomado especial cuidado com os chamados "***emails* de *phishing***", quando *emails* falsos são usados para tentar extorquir palavras-passe. A fim de reduzir os riscos provenientes da comunicação *online*, faz sentido guardar primeiro os anexos de correio eletrónico suspeitos e **analisá-los com um antivírus**.

Também existe o risco de se infetar o computador com *malware* ou de ser reencaminhado para *sites* de *phishing* quando se clica descuidadamente em ligações ou abre ficheiros que surgem em fóruns ou salas de *chat*. As identidades falsas ou a co-leitura indesejada de mensagens são outros exemplos de perigos que devem ser tidos também em conta.
Por conseguinte, é particularmente importante ler atentamente os regulamentos de proteção de dados dos fornecedores de comunicações *online* e nunca revelar dados pessoais ou sensíveis em *chats* e/ou fóruns.

Isto também se aplica quando se usam as redes sociais. É importante estar ciente de que, especialmente nas redes sociais, existe o perigo de se ser enganado por identidades falsas ou pela divulgação consciente ou inconsciente de informações falsas. Se detetares uma utilização indevida ou uma má conduta nas redes sociais, podes e deves denunciá-la ao prestador de serviços e às autoridades ou organizações apropriadas.

Co-funded by the
Erasmus+ Programme
of the European Union

As respostas corretas estão assinaladas a negrito

Situação: O que significa o termo "*email* falso"?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Os *emails* falsos são *emails* indesejados, que muitas vezes contêm *malware* enviado através de anexos.**
- **Os *emails* falsos fornecem frequentemente informações falsas ou infundadas.**
- **Os *emails* falsos podem nem sequer ter sido enviados pelo alegado remetente.**
- Os *emails* falsos são mensagens de correio eletrónico sem qualquer conteúdo. Estes *emails* em branco foram enviados intencionalmente ou como uma mensagem acidental.

Situação: Ao verificar a caixa de entrada do teu *email*, reparas que tens imensos *emails* novos. Qual dos seguintes casos é mais provável ser falso?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **O *email* promete um enorme prémio.**
- **É pedido com urgência que alteres os dados de *login* de uma plataforma.**
- O *email* não tem assunto.
- **O assunto inclui as palavras "aviso final".**
- **O *email* contém um número percetível de erros ortográficos.**
- **O *email* foi automaticamente movido para a pasta de *spam*.**
- O *email* foi enviado de madrugada.

Situação: Quais as medidas que podem ajudar a reduzir o risco de comunicações *online* via *email*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- **Ativar a visualização da extensão do ficheiro (por exemplo,. docx, .exe).**
- Desativar a visualização da extensão do ficheiro.
- **Usar definições de segurança apropriadas para impedir a execução de conteúdos ativos em programas de correio eletrónico.**
- **Verificar anexos suspeitos com um programa antivírus.**
- Só divulgar dados de utilizador se se conhecer muito bem as empresas que os estão a solicitar.

Situação: O que são salas de *chat* e o que são fóruns? Como é que as ferramentas diferem uma da outra?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- As salas de *chat* são muito adequadas para discussões em que nem todos os participantes têm de estar *online* ao mesmo tempo.
- Os fóruns são mais adequados para falar com os outros em tempo real do que as salas de conversação.
- **Podem trocar-se mensagens de texto tanto em salas de *chat* como em fóruns. Muitas vezes, também se podem trocar imagens, vídeos, links, ou ficheiros.**
- **Os *chatrooms* são mais adequados para comunicar com outras pessoas em tempo real do que os fóruns.**
- Embora seja possível conversar anonimamente ou sob um pseudónimo em salas de *chat* é necessário revelar o nome verdadeiro nos fóruns.

Situação: Os fóruns e salas de *chat* são ferramentas muito populares de comunicação *online*. No entanto, qual dos seguintes riscos podem surgir durante o uso destas ferramentas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- A utilização de *software* malicioso através da abertura de ficheiros partilhados em salas de *chat* ou fóruns.
- O redirecionamento para *sites* de *phishing* através do clique em *links* partilhados.
- Custos monetários muito elevados por causa de alguma troca de mensagens em fóruns.
- Alguém tentar enganar outros utilizadores fazendo uso de uma identidade falsa ou inventada.
- A intromissão e leitura por parte de terceiros de mensagens de *chat* enviadas em privado para uma pessoa.

Situação: Quais das seguintes medidas podem ajudar a reduzir o risco das comunicações *online* via fóruns e salas de *chat*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Ler os termos e condições gerais do serviço de comunicação.
- Bloquear os contactos que não se conhece.
- Partilhar apenas fotografias ou ficheiros que não tenham sido concebidos pelo próprio.
- Só permitir que alguém aceda ao computador pessoal se tiver uma foto de perfil e um nome de utilizador de confiança.
- Não abrir ficheiros recebidos de forma suspeita.

Situação: O que se deve fazer ao utilizar as redes sociais para evitar possíveis consequências negativas?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Aceitar o maior número possível de pedidos de amizade para parecer o mais popular possível para os outros.
- Verificar sempre as definições das redes sociais para proteção da privacidade.
- Não acreditar em toda a informação que aparece nas redes sociais.
- Se não gostas de alguém e gostarias de publicar comentários muito negativos sobre essa pessoa, tem cuidado para não usares o teu nome verdadeiro, especialmente se usares uma linguagem mais dura. Desta forma, poderás permanecer anónimo e não terás de temer consequências.

Situação: Estás a usar a tua conta nas redes sociais. Enquanto estas a ver as tuas redes sociais ficas em choque, descobres que alguém publicou um vídeo que mostra um grupo de adolescentes a intimidar e a abusar de uma rapariga tanto física como psicologicamente. Como deves reagir?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Deves denunciar o vídeo ao fornecedor do serviço (por exemplo, Facebook)
- Infelizmente, não há nada que se possa fazer. Talvez o vídeo não seja sequer real. Para evitares ser ameaçado, deves ignorar o mesmo.
- Deves denunciar o vídeo à polícia.
- Não conheces a vítima nem o agressor, pelo que não irás saber dar um nome concreto a ninguém e, portanto, não vale a pena interferires.