Proteção de Dados
https://www.uminho.pt/protecaodados
protecaodados@uminho.pt
Telefone: +351 253 510 006

Universidade do Minho

Título: Boas práticas de segurança informática para utilizadores

1. Âmbito e Objeto

As boas práticas propostas neste documento são a orientação do DPO a respeito de segurança informática dirigida a todos os utilizadores dos recursos informáticos da Universidade do Minho (UMinho)

2. Boas práticas de segurança informática

2.1. Considerações gerais

- A segurança informática é uma responsabilidade coletiva e individual.
- A manipulação ou o engano do utilizador é um dos principais meios de comprometimento inicial dos dispositivos e sistemas. Cada utilizador deverá sempre questionar e verificar a legitimidade e adequação das solicitações que recebe e dos *sites* que visita.
- A segurança informática pode perder-se em apenas uma oportunidade, pelo que, não podem haver exceções no que respeita à correta utilização dos recursos.

2.2. Correio Eletrónico

- Utilize o email institucional apenas para finalidades relacionadas com o seu trabalho na UMinho.
- Utilize o email institucional, e não outro, para tratar os assuntos relativos ao seu trabalho na UMinho.
- Verifique a proveniência das mensagens de email validando o endereço de email do remetente.
  a. Não confie simplesmente no nome do remetente porque é definido livremente, pode ser facilmente forjado.
  b. Tenha atenção a qualquer alteração na redação do endereço de email do remetente, a diferença de uma letra poderá corresponder a um remetente diferente.
  (ex: em www.rnicrosoft.com no lugar do "m" está um "r" e um "n")
- Suspeite sempre de mensagens despropositadas ou fora de contexto.
  a. Não abra ficheiros anexos ou ligações em mensagens desta natureza.
  b. Se a mensagem vier de um endereço que mereça credibilidade, confirme a legitimidade da mensagem junto do remetente. Preste atenção à autenticidade da resposta.
  c. Se o endereço do remetente lhe parecer suspeito reporte para csirt@uminho.pt.
- Suspeite de mensagens com ofertas ou ameaças que, em primeira análise lhe parecem dirigidas, mas que, em segunda análise não identificam mais do que o seu email e, eventualmente, o nome.
  a. Considere a possibilidade de que o que lhe é comunicado ou proposto seja falso.
  b. Não abra ficheiros anexos ou ligações.
  c. Reporte para csirt@uminho.pt.
- Suspeite de mensagens não solicitadas, por mais nobres que sejam as causas a que respeitem ou vantajosas as propostas que lhe façam.
  a. Não abra ficheiros anexos ou ligações.
  b. Verifique os factos diretamente no site da entidade proponente.
- Ignore quaisquer mensagens com orientações quanto à utilização de sistemas informáticos que não provenham dos endereços institucionais reconhecidamente com essas competências.
  a. Reporte para csirt@uminho.pt.
- Nunca responda a pedidos de cedência dos seus dados de acesso a sistemas ou serviços.
- Mensagens com anexos e ligações:
  a. Não abra anexos ou ligações em mensagens sem relevância para o seu trabalho;
  b. Verifique cuidadosamente a credibilidade das mensagens com ligações ou anexos que tenha de abrir. Confirme a legitimidade da mensagem junto do remetente. Preste atenção à autenticidade da resposta.
  c. Antes de abrir uma ligação, verifique o endereço de destino passando com o rato por cima, sem lhe clicar.
  d. Depois de abrir uma ligação e antes de qualquer ação verifique o endereço do site.
  e. Os endereços "curtos", como https://bit.ly/3Ny9U8V ou https://tinyurl.com/4xbmjtau, são completamente opacos quanto ao seu verdadeiro destino, só devem ser abertos em caso de muito elevada credibilidade do remetente e da mensagem, deve ainda ser verificada a legitimidade do destino acedido.
  f. Se algo lhe parecer errado reporte para csirt@uminho.pt.
- Mensagens a requerer informação:

a. Verifique cuidadosamente a credibilidade das mensagens que requeiram o envio de informação de acesso restrito.
b. Garanta, com um grau de certeza adequado à sensibilidade da informação solicitada, que o endereço de email que vai usar corresponde ao legítimo destinatário da informação a enviar.
c. Se necessitar de usar dados de contacto constantes em email, verifique se coincidem com os registos existentes na UMinho, ou junto de fontes oficiais da instituição se for o caso.
d. Se a informação a enviar for extensa ou sensível, dados pessoais de terceiros, ou outra com elevados requisitos de segurança e confidencialidade, a informação só deve ser enviada por email se estiver cifrada. A chave que decifre a informação deve ser trocada com o destinatário por um outro canal que não o email, com garantias suficientes de que o interlocutor nesse canal é o legítimo destinatário da informação.

- Não conserve informação sensível, de acesso restrito, ou informação sujeita a limitação temporal de conservação nas caixas de entrada, de saída ou de mensagens apagadas (lixo) do email.
- Alerte os seus colegas quando identifique mensagens fraudulentas para que estejam preparados se também forem visados.

2.3. Outras ferramentas de comunicação e colaboração

- Aplique os mesmos princípios enunciados para o email a outros instrumentos de comunicação e colaboração, com as devidas adaptações:
  a. utilize as ferramentas institucionais,
  b. verifique sempre o remetente e o destinatário,
  c. suspeite de mensagens despropositadas,
  d. seja prudente a abrir documentos e ligações, assim como a enviar informação.

2.4. Conta institucional de utilizador dos serviços digitais

- As ações realizadas nos serviços digitais da UMinho sob autenticação da conta institucional são da responsabilidade do seu titular.
- O direito de utilização da conta é intransmissível.
- O titular da conta deve zelar pela qualidade e confidencialidade da sua *password* e deve altera-la quando uma destas propriedades se perca.
- As *passwords* utilizadas nos serviços digitais da UMinho devem ser de utilização exclusiva nessas contas.
- As *passwords* não devem ser guardadas desprotegidas em suportes digitais ou físicos. As *passwords* guardadas em suportes digitais devem estar cifradas, as *passwords* em suporte físico devem guardar-se em local fechado de acesso restrito ao titular.
- As *passwords* devem ser longas, originais e improváveis. Uma frase com três palavras aleatórias, desconexas, com letras, números e símbolos, constituirá uma *password* forte.
- As *passwords* devem ter no mínimo 10 carateres.
- As *passwords* devem ter carateres de pelos menos três dos seguintes tipos: letras maiúsculas, letras minúsculas, algarismos, sinais de pontuação e símbolos.
- As *passwords* não devem ser constituídas por uma única palavra ou citação, mesmo que com alterações de alguns caracteres como “uM1nh0”.
- As *passwords* não devem conter informação pessoal.
- Caso suspeite da violação da sua conta institucional verifique se consta de violações de dados conhecidas em https://haveibeenpwned.com/

2.5. Incorporação e alienação de dispositivos e sistemas

- Todos os dispositivos e sistemas institucionais devem ser reinstalados de raiz antes de serem colocados ao serviço da UMinho.
- Todos os dispositivos e sistemas institucionais devem ser limpos de forma irreversível de quaisquer informações ou configurações quando terminem o seu serviço à UMinho.

2.6. Cópias de trabalho de informação institucional

- A conservação de informação institucional em equipamentos de utilização individual deve ser transitória, enquanto se encontre em situação de tratamento ativo. Terminado o tratamento ativo a informação deve ser atualizada no repositório institucional e a cópia no equipamento individual deve ser eliminada.
- Não copie informação institucional para sistemas ou serviços alheios à UMinho.

2.7.Cópias de segurança

- Toda a informação cuja perda constitua prejuízo para a UMinho deve ter pelo menos uma cópia de segurança periódica, preferencialmente automatizada.
- A informação em cópias de segurança deve estar sujeita a controlo de acessos não menos restrito que a informação original.

- Deve haver pelo menos uma cópia de segurança em dispositivo diferente da informação original. Esse dispositivo deve ter conetividade tão restrita quanto possível e controlos de acesso autónomos e diferentes daqueles da informação original.
- A eficácia do processo que efetua as cópias de segurança deve ser verificada regularmente.

2.8. Segurança dos dispositivos institucionais

- Os dispositivos institucionais devem ter alguma forma de controlo de acesso, que deve ser ativado em todas as ausências do seu utilizador.
- Os sistemas operativos e aplicações devem estar dentro do período de vida definido pelo produtor e ter instaladas as atualizações de segurança recomendadas pelo produtor.
  Os sistemas que não possam cumprir este requisito devem ser desligados da rede, ou ser alvo de outras medidas de mitigação atestadas por um especialista em segurança informática.
- Todos os dispositivos ligados a uma rede devem ter ativo um sistema antivírus e *firewall*.
- A utilização de privilégios elevados, como perfis de "Administrador" e "*Root*", deve ser restrita a operações de instalação e configuração dos dispositivos, efetuadas por pessoas com competência para o efeito. A utilização diária deverá ser feita com perfis de privilégios limitados.
- Todo o software instalado deve provir de fornecedores confiáveis e deve ser obtido de fontes oficiais.
- Não deverá conectar-se aos dispositivos institucionais qualquer outro dispositivo que não dê garantias suficientes da sua segurança.
- O acesso à Internet com dispositivos institucionais deve ser prudente, evitando a exposição a riscos desnecessários da utilização da Internet.
- Os navegadores (browsers) devem ser configurados para guardar os ficheiros descarregados e nunca para os abrir ou executar de forma automática, permitindo assim avaliar previamente a sua adequação.

2.9. Segurança dos dispositivos móveis

- Os dispositivos móveis, as unidades de armazenamento portáteis ou qualquer equipamento que possa ser extraviado, deve ter a informação sensível ou confidencial cifrada.
- O controlo de acessos dos dispositivos móveis deve ativar-se automaticamente após poucos minutos de inatividade.
- Os dispositivos móveis não devem ser deixados sem vigilância em locais onde haja risco de acesso indevido ou extravio.

2.10. Utilização de dispositivos pessoais

- Os dispositivos pessoais utilizados para aceder a informação institucional, incluindo o correio eletrónico, devem cumprir os mesmos requisitos de segurança enunciados para os dispositivos institucionais.
- Todos as configurações para acesso a informação institucional, assim como informações guardadas no dispositivo devem ser eliminadas de forma definitiva logo que deixem de ser necessárias.
- Os dispositivos pessoais com acesso a informação institucional não deverão ser partilhados com terceiros, pelo menos não sob a conta de utilizador que disponha do acesso.

2.11. Acesso remoto

- O acesso remoto a recursos da UMinho deve fazer-se sempre por meio de ligação VPN para que se protejam os dados transmitidos, por exemplo *passwords*.
- O acesso remoto a recurso da UMinho deve fazer-se através de dispositivos que deem garantias de estar livres de software malicioso, cumprindo os requisitos de segurança estabelecidos para os dispositivos institucionais.

2.12. Utilização de serviços *online*

- Não devem carregar-se informação e documentos institucionais sensíveis ou confidenciais, não cifrados, para serviços e plataformas *online* [1] com as quais a UMinho não tenha um contrato que garanta termos do serviço e confidencialidade da informação.
- Não devem descarregar-se ficheiros de fontes cuja idoneidade se desconhece.

2.13. Notificação de incidentes

- Os incidentes de segurança informática devem ser reportados sem demora à equipa de resposta a incidentes de segurança informática da UMinho (CSIRT.UMinho) para csirt@uminho.pt.
- As violações de dados pessoais deverão ser notificadas ao DPO de acordo com as instruções constantes na página da Proteção de dados: https://www.uminho.pt/protecaodados.

---

[1] Por exemplo: contas de correio eletrónico pessoais, serviços de transferência de ficheiros, serviços de processamento de PDFs, serviços de alojamento de ficheiros, etc..