BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

PÚBLICO - ALVO | TEMPO DE LEITURA | DIFICULDADE

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

COMO

Cuide dos dispositivos:

- Utilize de preferência dispositivos autorizados pela sua organização e, se os perder, informe o responsável de cibersegurança;
- Seja o único a utilizá-los – evite que terceiros os utilizem;
- Use apenas *pens* USBs confiáveis;
- Ative o bloqueio automático dos dispositivos e use PIN ou *password*;
- Utilize filtro no ecrã do portátil.

Cuide dos sistemas e dos dados:

- Garanta junto da sua organização que os dispositivos estão atualizados e têm o antivírus e a *firewall* ativados;
- Faça *backups* regulares para um dispositivo externo.

Cuide da navegação:

- Evite usar o Wi-Fi de espaços públicos e utilize sempre a VPN da sua organização;
- Navegue sempre em *websites* HTTPS;
- Altere a *password* do Wi-Fi doméstico depois da instalação;
- Garanta que o seu Wi-Fi doméstico tem uma *password* forte, secreta e altere-a regularmente;
- Altere o nome do seu Wi-Fi doméstico de modo a não ser facilmente identificado como seu;
- Escolha o modo de cifrar mais forte da sua rede Wi-Fi;
- Garanta que a rede da sua organização é segmentada de modo a proteger a rede interna.

Cuide da comunicação:

- Não abra *emails* ou SMS, nem clique em *links* ou anexos, desconhecidos;
- Cifre as comunicações sensíveis;
- Não partilhe informação profissional nas redes sociais.

O QUE CORRE BEM QUANDO AGE BEM

- Ajuda a manter a sua organização protegida de ciberataques;
- A informação sensível ou competitiva da sua organização fica mais segura;
- Evita ser responsável por um incidente de cibersegurança.

Em caso de dúvida, envie-nos um email ou telefone que nós esclarecemos.
Para aceder a mais documentação, consulte o nosso website: www.cncs.gov.pt
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

CNCS Centro Nacional de Cibersegurança PORTUGAL

BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

PORQUÊ O CUIDADO

Porque ao trabalharmos fora do contexto físico da nossa organização tornamos os sistemas e a gestão da informação mais vulneráveis, visto estarmos mais expostos a terceiros, quer em termos físicos, quer digitais.

SABIA QUE?

Os trabalhadores, voluntaria ou involuntariamente, são por vezes os principais responsáveis por ciberataques que afetam as suas organizações (*insider*). Na verdade, frequentemente, essa responsabilidade resulta mais da falta de cuidado do que de intenções maliciosas. É por essa razão que em cibersegurança se dá tanta importância ao fator humano. Por mais que as organizações estejam apetrechadas das melhores infraestruturas técnicas de proteção, basta um erro humano para colocar a cibersegurança em causa, nomeadamente através de ações como clicar num *link* com *software* malicioso, partilhar informação sensível com agentes mal intencionados ou em *websites* inseguros, perder dispositivos não bloqueados, utilizar *pens* comprometidas, aceder a Wi-Fi públicos ou não ter o Wi-Fi doméstico com uma *password* segura.

Os trabalhadores de algumas organizações, quer públicas, quer privadas, podem ser alvos apetecíveis para atividades de ciberespionagem. Quando a organização é privada e com fins lucrativos, normalmente o motivo é económico e prende-se com a espionagem industrial, visando obter informação privilegiada para a competitividade. Contudo, noutros casos, em geral ligados a organizações públicas, os motivos podem colocar em causa a segurança nacional.

A informação, profissional ou privada, que os trabalhadores expõem na Internet pode ser utilizada contra eles, em atos de engenharia social, como *phishing*, *smishing*, *vishing* ou *deep fake* de modo a levar estes trabalhadores, isolados em teletrabalho, a agir beneficiando o infrator, como seja fornecendo credenciais, fazendo transferências bancárias ou transmitindo outras informações sensíveis. Em muitas situações esta engenharia social atua simulando a identidade do CEO ou de outra chefia (*CEO fraud*) de modo a tornar-se mais credível e com autoridade.

Uma cadeia de ataque em cibersegurança inicia-se com um momento de reconhecimento, algo que pode passar pela simples recolha de informações sobre possíveis alvos de engenharia social. Por isso, é importante prevenir este tipo de situação mediante o conservadorismo na partilha de informações pessoais *online*. Em espaços públicos também é necessário ter cuidado, visto muita informação privilegiada poder ser recolhida através da visualização discreta de um monitor visível incautamente (*shoulder surfing*).

Quando se viaja, a condição de isolamento e exposição são intensificadas e podem ser vulnerabilidades percebidas por quem tem intenções maliciosas. Durante esses períodos, é muito importante vigiar os dispositivos de modo a evitar furtos ou perda.

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

CNCS Centro Nacional de Cibersegurança PORTUGAL

BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

DADOS

Num inquérito mundial (Cyberedgegroup), de 2018, 50,6% das organizações do setor da saúde e 47,3% das PME relataram que a sua principal preocupação de segurança é a ameaça interna.

Outro estudo (Forcepoint), em 2018, mostra que em 77% dos casos de *data breach*, a responsabilidade é de um *insider*.

Em 2018, 54% das empresas (Alertlogic) registaram um aumento da ameaça interna.

Um estudo (Broadcom), também de 2018, mostra que os dados mais vulneráveis à ameaça interna são as informações confidenciais de negócio (finanças, clientes, trabalhadores). Os ativos de Tecnologias de Informação mais vulneráveis são as bases de dados.

(ENISA Threat Landscape 2018 (2019): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

Nota: para um maior aprofundamento técnico dos melhores procedimentos de cibersegurança em teletrabalho, trabalho remoto e *bring your own device* (BYOD), consultar NIST Special Publication 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf)

GLOSSÁRIO

Antivírus

"Programa que monitoriza o computador ou a rede de modo a identificar tipos de *software* maliciosos e prevenir ou conter um incidente desse tipo."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

CEO Fraud:

"Ocorre quando um colaborador autorizado a fazer pagamentos é ludibriado [por alguém que se faz passar pela chefia da organização] no sentido de pagar uma fatura falsa ou realizar uma transferência não autorizada da conta bancária da organização."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

Ciberespionagem:

"Esta ameaça geralmente tem como alvo os setores industriais, as infraestruturas críticas e estratégicas em todo o mundo, incluindo entidades governamentais, transportes, provedores de telecomunicações, empresas de energia, hospitais e bancos. Foca-se na geopolítica, no roubo de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos."

(ENISA Threat Landscape 2018 (2019): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

Data Breach:

"Termo utilizado para designar um incidente resultante de uma fuga ou exposição de dados (incluindo informação sensível relacionada com organizações ou simples detalhes pessoais de indivíduos). Relaciona-se diretamente com os resultados de outras ciberameaças."

(ENISA Threat Landscape 2018 (2019): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

Deep Fake:

"Falsificações profundas, vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática."

(Desafios à Eficácia da Política de Cibersegurança da UE, TCE 2019: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf

Engenharia Social:

"Ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

Firewall:

"Porta que limita o acesso entre redes de acordo com a política de segurança local."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

HTTPS:

"O protocolo HTTPS (Hypertext Transfer Protocol Secure) é uma variante do HTTP (Hypertext Transfer Protocol) padrão que adiciona uma camada extra de segurança aos dados enviados, através do protocolo SSL (Secure Socket Layer) ou TLS (Transport Layer Security). O HTTPS permite utilizar uma comunicação cifrada e uma conexão segura entre o utilizador e o servidor principal."

(traduzido de Techopedia: https://www.techopedia.com/definition/5361/hypertext-transport-protocol-secure-https)

Insider:

"A ameaça interna pode existir em todas as empresas ou organizações. Qualquer colaborador atual ou ex-colaborador, sócio ou fornecedor, que tenha, ou tenha tido, acesso aos ativos digitais da organização, pode abusar, voluntaria ou involuntariamente, desse acesso. Os três tipos mais comuns de ameaças internas são:

BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

insider malicioso, que age intencionalmente; *insider* negligente, que é desleixado ou não está em zconformidade com as políticas e instruções de segurança; e *insider* comprometido, que age involuntariamente como instrumento de um atacante real."

(ENISA Threat Landscape 2018 (2019):
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

Phishing:

"É o mecanismo de criação de mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado, 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os destinatários de *emails* ou mensagens de *phishing* para que estes abram anexos maliciosos, cliquem em URLs inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas, façam transferências de dinheiro, etc.."

(ENISA Threat Landscape 2018 (2019):
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018)

Shoulder surfing:

"A prática de espiar o utilizador de uma caixa multibanco ou outro dispositivo eletrónico com o objetivo de obter um número de identificação pessoal, uma *password*, etc."

(traduzido de Lexico: https://www.lexico.com/definition/shoulder_surfing)

Smishing:

"Ocorre quando um telemóvel recebe um SMS de uma pessoa ou entidade falsas. O utilizador de telemóvel incauto responde a um SMS falso e visita um URL, fazendo o *download* inadvertido de *software* malicioso e instalando um *trojan* sem o seu conhecimento. O *phishing* procura extrair informação útil, por isso, no caso do *phishing* através de SMS [*smishing*], o *trojan* recolhe a informação armazenada no telemóvel e transmite-a à pessoa que o criou."

(traduzido de Techopedia: https://www.techopedia.com/definition/24898/sms-phishing)

Software malicioso:

Programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms:
https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)

BOAS PRÁTICAS DE CIBERSEGURANÇA EM TELETRABALHO

OBJETIVO: GARANTIR A CIBERSEGURANÇA DO TELETRABALHO OU TRABALHO À DISTÂNCIA

Vishing:

"Uso de mensagens de voz para roubar identidades e recursos financeiros. O termo resulta da combinação de *voice* e *phishing*."

(traduzido de Techopedia: https://www.techopedia.com/definition/4159/vishing)

VPN (Virtual Private Network):

"Uma rede virtual, sobreposta às redes físicas existentes, que providencia comunicações seguras em túnel para dados e outras informações transmitidas entre redes."

(traduzido de NIST IR 7298 Revision 2, Glossary of Key Information Security Terms: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf)