Temática – Conhecer a Cibersegurança?

Conceito

O conceito de Cibersegurança, ao longo dos tempos, até motivado pela própria noção de transformação digital, tem sido alvo de diversas interpretações:

- Pode ser entendido como o conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação;

- Por outro lado, ser definido como o sentimento de segurança percecionado pelas pessoas quando usam a Internet e as tecnologias digitais.

Fonte: Adaptado de CNCS.gov.pt – 07.Abr.2022.

Boas práticas em termos de Cibersegurança

Os 5 pontos críticos

Para saber como agir em casa, no trabalho ou em viagem e de forma preventiva. Estes "pontos críticos" correspondem a comportamentos que nos ajudam a proteger das ciberameaças. Para que estes "pontos críticos" sejam tratados com cuidado, iremos elencar um conjunto de boas práticas a que devemos obedecer.

1. Palavra-passe

Um dos "pontos críticos" que identificamos é a palavra-passe e o comportamento que devemos estimular é a capacidade de "complicar", uma vez que o nosso principal objetivo deverá ser tornar a captura da palavra-passe mais difícil e complexa.

Assim, para podermos criar uma palavra-passe, que complique e não simplifique a possibilidade de ser descoberta, apresentamos a "Regra das 8 Complicações".

A palavra-passe

1) deve ser secreta, e não transmitida a ninguém;
2) deve ser complexa e memorizável, difícil de descobrir e não registada em documentos acessíveis – pode ser uma frase, com vários tipos de caracteres, em vez de uma palavra;
3) deve ser alterada sempre que se desconfie que foi comprometida;
4) deve ser usada numa só plataforma, evitando comprometimento de vários serviços no caso de ser descoberta;
5) se possível, utilizar autentificação de duplo fator, garantindo a

segurança no caso de comprometimento;
6) deve ser alterada sempre por defeito, evitando *palavras-passe* indicadas pelos serviços e produtos adquiridos;
7) deve ser guardada num gestor *offline* com base de dados cifrada, que permite gerir uma variedade grande de palavras-passe com risco reduzido de perda ou esquecimento; 8) não deve ser guardada em *browsers,* dado que existem métodos relativamente simples para descobrir estas palavras-passe.

Ter uma palavra-passe forte e robusta é fundamental para proteger a informação pessoal e corporativa. O comprometimento da palavra-passe pode envolver o roubo de identidade e a violação de dados.

2. E-mail

O segundo "ponto crítico" é o e-mail e o comportamento que devemos estimular é a desconfiança em relação aos e-mails que recebemos, assim como aos conteúdos dos mesmos.

O e-mail é um ponto nevrálgico de muitos ataques. É a porta de entrada para os sistemas privados e/ou de empresas, e está muito associado ao *ransomware* (tipo de *malware* que infeta os sistemas informáticos e cifra os seus dados de modo a que a vítima não consiga utilizar os mesmos, sendo alvo de chantagem para pagar um resgate em troca da chave de decifra).

Desta forma, para capacitarmos comportamentos de desconfiança, apresentamos a "Regra das 6 desconfianças":

1) abrir apenas e-mails de origem conhecida, os e-mails desconhecidos podem ser maliciosos;
2) caso abra um email desconhecido, não clicar em nenhum link ou anexo, dado que são pontos críticos para a instalação de software malicioso;
3) verificar o endereço e a veracidade dos e-mails conhecidos, mesmo os e-mails aparentemente conhecidos podem estar comprometidos (devemos estar atentos a pormenores desajustados, como caracteres diferentes, imagens, etc.);
4) não enviar informação sensível/confidencial por e-mail, mesmo que o destino seja de confiança, o envio pode ser comprometido por terceiros, a não ser que se use PGP (*Pretty Good Privacy*);
5) identificar o SPAM para que o sistema faça uma seleção prévia, a identificação é a melhor maneira de evitar a receção deste tipo de e-mail, potencialmente malicioso; 6) terminar sempre a sessão quando finalizar a utilização do e-mail, uma sessão por encerrar pode ser acedida por alguém que abra o *browser* posteriormente.

3. Redes Sociais

O terceiro "ponto crítico" são as redes sociais e o comportamento a estimular é a preservação da vida privada.

A taxa de utilização das redes sociais atinge, presentemente, valores bastante significativos e os comportamentos de exposição da vida e dados pessoais continuam a ser um fator crítico a evitar. Furto de identidade, engenharia social, entre outros fenómenos consequentes desta exposição têm que ser contrariados. Apresentamos os 5 "A não fazeres" nas Redes, para estimularmos a preservação da vida privada:

1) não aceitar convites de desconhecidos, uma vez que aceitar estes convites é arriscar

uma ligação a alguém com intenções maliciosas;

2) não indicar telefone ou moradas no perfil, estes dados podem ser usados em ações de engenharia social;
3) não partilhar locais, imagens de crianças ou dados sensíveis, dado que além de estes dados também poderem ser usados para a engenharia social, podem ainda servir para assaltos ou pornografia infantil;
4) não partilhar notícias falsas – verificar sempre a fonte, em caso de dúvida (apenas fontes reconhecidas devem ser legitimadas);
5) não clique em *posts* suspeitos – podem ser *phishing*, que também existe nas redes sociais (devemos usar as mesmas regras de proteção que usamos para o e-mail).

Fique a saber ainda:

- aquilo que publica pode ser usado por terceiros, uma vez que está acessível a desconhecidos por diversos canais;
- por cada gosto ou partilha realizado por si, é criado um perfil utilizável em plataformas que vendem os dados a empresas de publicidade, que fazem microsegmentação;
- quando acede a plataformas usando contas de redes sociais, partilha os seus dados, visto que está a autorizar o acesso destas plataformas às suas redes sociais;
- ao colocar uma imagem nas redes sociais, abdica dos direitos sobre a mesma. As redes sociais ficam com os direitos de autor da imagem publicada (nada é gratuito nas redes sociais, troca-se o serviço por dados e conteúdos que disponibilizamos).

4. Hardware

O quarto "ponto crítico" é o *hardware* e o comportamento a promover é o de bloquear os dispositivos a terceiros.

A recomendação que sugerimos para este comportamento é a utilização da "*Hardware Checklist*":

- Cobrir câmaras e desativar microfone, visto que através de acessos maliciosos ao computador é possível ativar estas funções e ter acesso a imagem e som em direto;
- Ativar bloqueio e não deixar os dispositivos desbloqueados, para evitar ações maliciosas de estranhos;
- Usar palavra-passe e limite de tentativas, para proteger os dados no caso de furto ou perda;
- Evitar olhares indiscretos, ao tratar informação confidencial, quando os ecrãs estão em espaço público ou visíveis a terceiros;
- Em viagem, identificar e vigiar dispositivos;
- Em organizações, cifrar informações e proteger perímetro, evitando a ação, voluntária ou não, de *insiders*;
- Proteger portas USB, estas são um ponto de entrada para ações maliciosas, existem métodos para controlar o perímetro e programas que definem o acesso permitindo-o apenas a alguns dispositivos - no limite, é possível desativar estas portas;
- Não usar *pen* USB desconhecida, pode transportar *malware*.

5. Navegação

O quinto e último "ponto crítico" é a navegação e o comportamento a seguir é o de prevenir a navegação por "sítios" maliciosos.

A utilização de Wi-Fi pública não é segura, a não ser que use uma VPN, uma vez que é

possível ficar exposto a terceiros. Também é necessário ter cuidado com as Apps que instala nos seus dispositivos.
Apresentamos as "Apptitudes" certas para se proteger de Apps maliciosas:

1) usar apenas plataformas reconhecidas para instalaçãodeApps*;*
2) verificar as *reviews*, pontuação e escolhas do editor - podem dar-nos indicações sobre a segurança da App;
3) não instalar Apps duvidosas, que estejam fora das plataformas conhecidas ou que levantem suspeitas;
4) denunciar Apps fraudulentas, para que outros não sejam vítimas;
5) não autorizar o acesso a funcionalidades desnecessárias - os dados dos utilizadores podem ser comercializados.

Deixamos também um conjunto de "Avisos à navegação" para que possa "surfar" a Internet em segurança:

- Use *firewall*, pois permite selecionar o tráfego seguro e evitar o inseguro com base em regras estabelecidas;
- Considere que endereços com "http**s**" são mais seguros, por se tratar de uma garantia de segurança adicional ao "http", cifrando a informação trocada;
- E-Banking: confirmar a autorização do Banco de Portugal ao Banco online que utiliza;
- Compras *online*: desconfiar de ofertas demasiado boas, recolher informação sobre o vendedor, usar formas de pagamento seguras (carteiras digitais, cartões temporários) e guardar o registo das transações;
- Acompanhar a navegação das crianças, elas são um elo mais fraco. É importante conhecer o uso que fazem da Internet e com quem interagem - se necessário, bloquear o seu acesso a algumas plataformas.

Por último, não podíamos deixar de referir, o aviso que é transversal a todos os pontos críticos até aqui mencionados: manter todos os programas e em particular o antivírus atualizados. As atualizações fazem correções de vulnerabilidades, protegendo de ameaças identificadas e eventualmente massificadas.
Não esquecer! Os hábitos de ciber-higiene são fundamentais para a segurança e só dependem de cada um de nós.

Fonte: Adaptado de NAU.edu.pt – 07.Abr.2022.