BIM

Boletim Informativo Mensal

Comunicar para Educar

Nº 05 – Junho/2020

Importância do uso de senhas seguras

Da mesma forma que uma chave dá acesso a uma residência, a um compartimento ou, até mesmo, a uma gaveta, as senhas digitais muitas vezes são a nossa “chave” para acesso a um determinado dispositivo digital, a um sistema computacional, a e-mails etc.

Agora, imagine que a chave que dá acesso a sua casa esteja sempre em local acessível por todos! Ou que você esqueceu de usá-la, tendo deixado sua residência com acesso facilitado a estranhos.

Você se sentiria seguro?
Acreditamos que não...

De modo semelhante a nossa casa, o ambiente computacional e as ferramentas digitais às quais temos acesso dispõem de mecanismos de segurança, para que se possa utilizá-los — por exemplo, as senhas!

Portanto, trate suas senhas com máximo cuidado e busque seguir, ao menos, as seguintes recomendações:

- não compartilhe sua senha — ela é somente sua, e deve ser de uso pessoal e intransferível;

- não deixe suas senhas escritas em local de fácil acesso, para evitar seu uso indevido por terceiros; e

- crie senhas fortes, elas são mais difíceis de serem quebradas, por tentativas não autorizadas — use caracteres especiais (Ex.: *, &, $, #), e evite algo óbvio, semelhante a “123senha”.

Para maiores informações de como se proteger no ambiente virtual acesse o *site:* www.ctir.gov.br.

Você também pode acessar os endereços de nossos parceiros:

- https://cert.br/
- https://www.rnp.br/

Engenharia Social x Segurança da Informação

A engenharia social é uma prática usada por indivíduos de má-fé, para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar, ou obter informações sigilosas e importantes.

É um golpe antigo, que se manifesta em todas as áreas da vida; é um erro pensar que é algo que você só vê no mundo on-line. A engenharia social é baseada na interação humana, e é conduzida por pessoas que usam o engano, para violar os procedimentos de segurança que normalmente deveríamos ter seguido.

O engenheiro social utiliza alguns meios para atacar — fique atento!

Ele pode realizar ligações para a vítima, fingindo sequestrar um ente querido, e pedir dinheiro, via transferência bancária; pode enviar e-mails falsos, para induzir você a clicar em links que instalarão vírus, talvez do tipo “cavalo de troia”, ou redirecionarão você para páginas falsas, que capturam dados digitados. O vasculhamento do lixo também é um dos métodos desse criminoso, para conseguir acessar informações sensíveis, pois nem todos utilizam máquinas fragmentadoras ou trituradoras de papel, para que os diversos documentos sigilosos não sejam recuperados por pessoas mal-intencionadas.

A proteção contra a engenharia social é um processo de conscientização sobre segurança da informação. Listamos alguns hábitos que devemos seguir:

- não forneça suas senhas, elas são pessoais e intransferíveis;
- descarte corretamente material que se acha inútil; triture os documentos, se não possuir trituradora, rasgue, e deposite as partes em diversas lixeiras;
- não deixe em cima da mesa, ou expostos, documentos com grande facilidade para alguém se apoderar ou ter acesso, principalmente, se as portas ou janelas ficam abertas;
- ao se ausentar da mesa ou da estação de trabalho, não deixe o computador ligado exibindo informações confidenciais; e
- não clique em links desconhecidos, nem baixe arquivos duvidosos em seu computador ou celular — o uso de um antivírus é recomendável.

Sendo assim, todos devemos ficar atentos, para não expor informações que possam ser utilizadas maliciosamente. Paranoias e neuroses à parte, todo cuidado é pouco!...

BIM
Boletim Informativo Mensal
Comunicar para Educar
Nº 05 – Junho/2020

Falamos em edições anteriores que o Posto de Controle (PC) é um local no órgão público ou privado onde as informações classificadas em qualquer grau de sigilo são armazenadas e controladas.

Vamos conhecer hoje um pouco mais sobre a **qualificação técnica mínima requerida ao PC**?

O PC deve, dentre outras qualificações:

- estar localizado em área de acesso restrito;
- possuir meios de armazenamento de documentos físicos e eletrônicos com nível de segurança compatível com os graus de sigilo e o volume;
- possuir estrutura física adequada para o armazenamento e preservação dos documentos físicos e eletrônicos;
- possuir suas redes de dados e seus sistemas de tecnologia da informação adequadamente protegidos de ataques eletrônicos;
- possuir protocolo exclusivo para documentos classificados e, quando necessário, para Documentos Controlados;
- possuir restrição ao uso de máquinas fotográficas, gravadores de vídeo e de áudio, ou similares, tais como câmeras de dispositivos móveis, no interior de suas instalações;
- possuir quadro de pessoal capacitado para o tratamento de informação classificada; e
- possuir recurso criptográfico para armazenamento e transmissão da informação classificada em conformidade com a Instrução Normativa GSI/PR nº 3, de 2013.

Todas as características do Posto de Controle são reguladas pelo item 8.5 da Norma Complementar nº 01, de 27 de junho de 2013. Para saber mais informações sobre esse assunto ou outras informações sobre segurança da informação acesse http://dsic.planalto.gov.br/

Já ouviu falar em ***SOFTWARE* DE CONTROLE PARENTAL**?

São ferramentas utilizadas para auxiliar na segurança das crianças e dos adolescentes na internet. Os chamados controles parentais estão presentes em smartphones, computadores, roteadores, e até em videogames — mas poucos usam!

Em que esses softwares podem auxiliar?

1. Permitem restringir os sites que podem (ou não podem) ser acessados.
2. Definem limites, como o tempo máximo de uso por dia, horário de dormir e regras específicas para dias úteis e de finais de semana.
3. Permitem definir quais os aplicativos que as crianças podem baixar e instalar; ou, ainda, os filmes que elas podem assistir; e os livros que podem ler.
4. Controlam o uso das redes sociais.
5. Impedem a troca de senha.
6. Mostram o histórico de atividades, incluindo sites visitados e aplicativos utilizados.
7. Permitem definir filtros, de acordo com a classificação etária do conteúdo.

É possível configurar o Controle Parental em sites de pesquisa (Google, Yahoo, Bing), no sistema do computador (Windows, OS X, Linux, etc.), nos dispositivos móveis (Android, iOS, Windows), videogames e roteadores. Em uma rápida busca na internet, você conseguirá acessar tutoriais que ensinam o passo a passo da instalação desses softwares, muitos gratuitos.

Sabemos que nada substitui a atenção, o diálogo, e a mediação dos pais, porém, é possível utilizar a tecnologia a favor dos pais, para ajudar a preservar as crianças dos riscos da internet.

Fonte: http://dsic.planalto.gov.br/ https://www.ctir.gov.br/
Editorial/redação/diagramação: DSI Sugestões: asscom.dsi@presidencia.gov.br