SEGURANÇA DA INFORMAÇÃO

eBook 2

O comportamento seguro na internet é uma forma de comportamento que envolve práticas de segurança para proteger a privacidade, a identidade e os dados pessoais na internet, com o objetivo de minimizar os riscos e proteger contra ameaças cibernéticas, tais como malware, phishing, hacking e roubo de identidade.

Comportamento seguro na Internet

Um comportamento seguro na internet envolve uma série de práticas, incluindo criar senhas fortes e únicas e alterá-las regularmente.

- Atualizar regularmente os sistemas operacionais e softwares com as últimas correções de segurança.
- Manter softwares de segurança atualizados, como antivírus e firewall.
- Evitar clicar em links suspeitos ou em e-mails de remetentes desconhecidos.
- Evitar fornecer informações pessoais ou confidenciais em sites não confiáveis.
- Verificar a segurança de sites antes de fornecer informações pessoais, especialmente quando se tratar de transações financeiras.
- Utilizar redes Wi-Fi seguras e criptografadas, especialmente ao se conectar a serviços financeiros ou bancários.
- Não compartilhar informações pessoais ou fotos em redes sociais que possam comprometer a privacidade.
- Não baixar arquivos de origem desconhecida ou de fontes ou remetentes não confiáveis.
- Manter o backup regular dos dados em dispositivos pessoais para minimizar a perda de informações em caso de roubo ou perda.

Senhas seguras

Com a crescente dependência da tecnologia, as senhas tornaram-se uma parte crucial da segurança da informação das empresas. Senhas fracas ou comprometidas podem colocar em risco os dados e as informações confidenciais das empresas. Por isso, é importante seguir algumas boas práticas em geral sobre senhas seguras.

Senhas longas
Quanto mais longa a senha, mais difícil torna-se o acesso de terceiros.

Complexidade
Uma senha segura deve ter uma mistura de letras maiúsculas e minúsculas, números e caracteres especiais, como símbolos e pontuação.

Informações pessoais
Senhas que tem informações como datas de aniversário, nomes de familiares, endereços ou números de telefone são fáceis de serem descobertas por hackers.

Senhas comuns
Senhas comuns como "123456", "password" e "qwerty" são facilmente descobertas e devem ser evitadas.

Compartilhar senhas
Senhas são como chaves, elas não devem ser compartilhadas com ninguém.

Atualizar as senhas
É recomendável que as senhas sejam atualizadas a cada três meses.

Autenticação
A autenticação multifator é um método de segurança em que o usuário fornece duas ou mais formas de autenticação para acessar uma conta.

Phishing
O *phishing* é uma técnica usada por hackers para obter informações confidenciais, como senhas.

Monitorar as senhas
É importante monitorar as senhas regularmente para garantir que não tenham sido comprometidas ou vazadas.

Proteção de dados

Além das boas práticas com as senhas, existem outras que podem ajudar a proteger os dados das empresas.

A Criptografia, que é uma técnica que transforma dados em um formato ininteligível para pessoas não autorizadas. É importante criptografar os dados confidenciais, como informações de clientes e senhas. A criptografia também deve ser usada ao transmitir informações pela internet.

O Backup, onde os backups regulares ajudam a garantir que os dados da empresa estejam protegidos contra perda ou roubo.

O Monitoramento de acessos suspeitos, porque é importante monitorar os acessos aos sistemas e identificar aqueles que forem suspeitos ou não autorizados.

E o controle de permissões de acesso, que é fundamental para limitar o acesso a informações confidenciais e evitar possíveis violações de segurança.
Por exemplo, muitas empresas garantem que os funcionários têm acesso somente às informações necessárias para desempenhar suas funções, e que o acesso seja revogado imediatamente quando o funcionário deixa a empresa ou muda de função.