Informações sobre senhas

IoTSafety

Grande parte dos ataques virtuais ocorre em função de falhas humanas. Por melhor que seja a política de segurança e privacidade de um empreendimento, o comprometimento de contas ainda é a principal fonte de entrada de softwares maliciosos em meios digitais. Os malwares são softwares maliciosos que têm como objetivo se infiltrarem em um computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações. Além desses malwares, ataques conhecidos como Phishing, utilização de vírus e ameaças físicas, existem e causam bastante estrago nas organizações.

Para evitar que esse tipo de ataque tenha sucesso, além das ferramentas de alerta nativas de cada sistema, é ideal investir em senhas complexas, que ampliam o tempo necessário para um sistema computacional conseguir obter um acesso forçado a uma conta.

Algumas dicas são:

- Mantenha senhas diferentes para cada tipo de site, assim como um conjunto de logins diferenciados para redes sociais e sites de e-commerce;
- Troque as senhas regularmente;
- Não utilize senhas com palavras comuns ou que tenham termos relacionados a você;
- Crie senhas fáceis de lembrar, mas com ao menos oito caracteres;
- Utilize letras maiúsculas, letras minúsculas e números;
- Não tenha as suas senhas anotadas em um papel ou bloco de notas;
- Utilize um gerenciador de senhas sempre que possível;
- Opte por métodos de autenticação de dois passos.