CYBERSECURITY AWARENESS MONTH

SEE YOURSELF IN CYBER (VOCÊ NO CIBERESPAÇO)

Todos desempenham um papel na segurança cibernética, independentemente do seu cargo.

Faça a sua parte para proteger a cibersegurança da sua empresa seguindo quatro ações principais.

ATIVE A AUTENTICAÇÃO MULTIFATOR

Também conhecida como "autenticação de dois fatores" e "verificação em duas etapas", a autenticação multifator é uma medida de segurança que exige que qualquer pessoa que entre em uma conta passe por um processo de duas etapas para comprovar a identidade. Isso faz com que seja duas vezes mais difícil para os criminosos acessarem uma conta on-line. Ao adicionar apenas uma simples etapa ao fazer login em uma conta, a autenticação multifator aumenta muito a segurança da conta.

USE SENHAS FORTES

Se você quiser manter as suas informações seguras, as senhas são muito importantes. Aqui temos algumas maneiras simples de proteger as contas utilizando práticas aprimoradas de senha. Independentemente da conta, todas as senhas devem ser criadas considerando estes três elementos.

- Longa – Pelo menos 12 caracteres
- Única – Cada conta precisa de uma única senha exclusiva
- Complexa – Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Alguns sites inclusive permitem adicionar espaços.

ATUALIZE O SOFTWARE

Sempre mantenha o seu software atualizado quando as atualizações estiverem disponíveis – e não demore. As atualizações corrigem problemas gerais de software e oferecem novos patches de segurança que os criminosos podem aproveitar para entrar nos sistemas. Ao baixar uma atualização de software, obtenha-a apenas junto à empresa responsável pela criação. Nunca use versões de software hackeadas, pirateadas ou não licenciadas pois elas geralmente contêm malware e causam problemas em vez de os resolver.

RECONHEÇA E DENUNCIE CASOS DE PHISHING

Os sinais podem ser sutis, mas assim que você reconhecer uma tentativa de phishing, poderá evitar cair nela. Para ajudar você a identificar claramente essas tentativas, aqui temos algumas dicas rápidas sobre o conteúdo de um e-mail falso de phishing: oferece algo bom demais para ser verdade; linguagem urgente, alarmante ou ameaçadora; péssima redação, com erros ortográficos e gramática ruim; saudações ambíguas ou muito genéricas; solicitações de envio de informações pessoais; urgência para clicar em hiperlinks ou anexos desconhecidos; solicitações de negócios estranhas ou abruptas; o endereço de e-mail do remetente não corresponde à empresa de origem.

MAUSER
Packaging Solutions