Quais são as suas responsabilidades para manter a cibersegurança

Esteja ciente dos riscos digitais

A primeira linha de defesa em cibersegurança é a conscientização. Todos devem estar cientes das ameaças cibernéticas e das melhores práticas de segurança.
Portanto, é importante que todos os funcionários participem de treinamentos regulares em cibersegurança. Esses treinamentos ajudam a entender as ameaças cibernéticas, como phishing, malware e engenharia social, e como evitá-las.
Esteja sempre de olho nas notícias e atualizações relacionadas à cibersegurança. Isso pode ajudar a entender as ameaças emergentes e como proteger nossos sistemas contra elas.

Mantenha seus dispositivos atualizados

Manter nossos sistemas e software atualizados é essencial para evitar vulnerabilidades que os cibercriminosos possam explorar. Sempre que receber notificações de atualizações para sistemas operacionais, aplicativos ou dispositivos, certifique-se de aplicá-las imediatamente.
Familiarize-se com nossa política de aplicação de correções e os prazos estabelecidos para a aplicação de correções críticas. Cumprir esses prazos é essencial para manter nossos sistemas seguros.
Você também pode manter um registro das datas de atualização de todos os ativos de TI que você utiliza. Isso ajuda a garantir que nada seja esquecido.

Gerenciamento de senhas e acessos

Senhas são uma parte crucial da cibersegurança, e todos nós temos um papel a desempenhar na criação e proteção delas.
Ao criar senhas, certifique-se de que sejam fortes, incluindo letras maiúsculas, minúsculas, números e caracteres especiais. Evite senhas óbvias, como "123456" ou "senha".
Nunca compartilhe suas senhas com colegas de trabalho, amigos ou familiares. As senhas são pessoais e confidenciais.
Sempre que possível, ative a autenticação de dois fatores em suas contas. Isso adiciona uma camada extra de segurança, mesmo que alguém saiba sua senha. Por fim, considere o uso de um gerenciador de senhas confiável para armazenar e gerar senhas seguras. Isso pode facilitar o gerenciamento de várias senhas de forma segura.

Previna-se contra o Phishing

O phishing é uma das ameaças mais comuns. Aprenda a identificar e evitar emails e mensagens suspeitas. Desconfie de emails não solicitados, especialmente aqueles que solicitam informações pessoais ou financeiras. Antes de clicar em links ou abrir anexos, verifique o remetente do email. Os hackers frequentemente se passam por fontes confiáveis.

Relate atividades de phishing

Se você receber um email suspeito, relate à equipe de segurança cibernética. Não tente lidar com isso por conta própria.

Reporte atividades suspeitas

Se você notar atividades suspeitas em nossos sistemas, não hesite em relatar imediatamente à equipe de segurança cibernética. Isso inclui e-mails suspeitos, mensagens incomuns ou comportamento não autorizado nos sistemas.

Uso Responsável da Internet e Dispositivos

Seu comportamento online e o uso de dispositivos pessoais também afetam nossa segurança cibernética. Siga as diretrizes estabelecidas para o uso de dispositivos pessoais no ambiente de trabalho. Certifique-se de que esses dispositivos estejam protegidos por senhas e evite acessar redes Wi-Fi públicas não seguras.
Evite fazer downloads de software ou aplicativos de fontes não confiáveis. Use apenas fontes oficiais e verificadas. A adoção de uma navegação segura ajuda a evitar infecções por malware.
A segurança cibernética é uma responsabilidade compartilhada. Cada um de nós desempenha um papel fundamental para manter a cibersegurança da nossa organização.
Ao estar ciente das ameaças, proteger suas senhas, manter sistemas atualizados, prevenir phishing e usar a internet e dispositivos de forma responsável, você está contribuindo para a defesa dos nossos ativos digitais.