Microsoft

Guia de conversação de segurança cibernética K-12

Ajude pais, professores, administradores escolares e responsáveis a ter conversas que ensinam os alunos K-12 sobre práticas cibernéticas seguras.

Por que é importante?

Os alunos são especialmente vulneráveis ao roubo de identidade, pois alguns podem não descobrir por anos até solicitarem um cartão de crédito ou empréstimo de carro. Além disso, os hackers geralmente veem os alunos como caminhos para as redes escolares, permitindo que eles roubem informações sobre professores, funcionários e pais.

Pontos-chave a discutir

Por que você não deve clicar em links desconhecidos

- Links desconhecidos vêm em todas as formas, incluindo mensagens de texto, e-mails, mecanismos de pesquisa, sites, postagens de mídia social, mensagens diretas e muito mais
- Às vezes, os hackers tentarão fazer amizade com você sob falsos pretextos ou se passarão por um membro da família, amigo, professor ou figura de autoridade para que você compartilhe informações com eles (isso é chamado de engenharia social)
- Clicar nesses links pode ter consequências que afetam diretamente sua vida, arruinando o dispositivo que você ama ou até prejudicando suas amizades se for hackeado e falsificado

Algumas bandeiras vermelhas de mensagens de phishing

Uma mensagem de phishing pode ter qualquer combinação desses problemas

- O phishing por SMS (ou SMSishing) é um grande problema para os alunos do ensino primário e secundário.
- Fontes legítimas podem escrever palavras incorretamente ou ter erros às vezes, mas tenha cuidado ao ver erros nas mensagens enviadas a você.
- Sempre passe o mouse sobre um link (incluindo e-mails) antes de clicar nele no seu computador para ver para onde ele irá
- Ameaça e urgência são muitas vezes transmitidas na mensagem para te assustar a e instigar você a agir antes de que possa verificar se o link é Seguro
- Sempre desconfie de mensagens ou chamadas que solicitem informações confidenciais (como credenciais de login)
- Para te enganar, os hackers às vezes oferecem recompensas falsas por entregar suas informações

Por que você deve evitar anúncios fraudulentos

- Os anúncios são pagos para serem colocados à sua frente e, às vezes, os hackers pagam para criar anúncios fraudulentos que coletam seus dados pessoais e invadem sua privacidade
- Cuidado com as bandeiras vermelhas comuns de phishing nesses anúncios fraudulentos e preste atenção especial ao link

É importante falar e obter ajuda se você clicar no link errado

- Enfatize que pedir ajuda não será punido ou repreendido. (Recomendamos uma configuração de autorrelato sem consequências, quando possível)
- Se você clicar em um link malicioso, sua vida não acabou! Você só precisa dizer a um adulto
- Uma vez que os adultos estejam envolvidos, eles podem tomar medidas para corrigi-lo
- Mas pode ser difícil de consertar, então tenha cuidado ao clicar!

Microsoft

Exemplos de quando estar mais atento!

Esses são cenários comuns em que um aluno pode ser alvo de uma tentativa de phishing. Esses exemplos são separados por faixa etária, mas você pode escolher os cenários mais relevantes para seus alunos.

Elementar

- Informações de pesquisa para um trabalho de aula
- Pesquisa de cursos de tutoria de matemática online
- Pesquisas de vídeos online e informações não verificadas em trabalhos escolares
- Enviar uma mensagem para um professor com uma pergunta

Secundário

- Encontrar um número de atendimento ao cliente
- Diferenciar anúncios e postagens orgânicas nas mídias sociais
- Receber uma mensagem solicitando que você digite sua senha ou ameaçando bloqueá-lo de sua conta
- DM com um link desconhecido e a outra pessoa pedindo para você clicar no link
- Procurar um emprego de verão e candidate-se a uma empresa fraudulenta
- Pesquisar e inscreva-se na faculdade ou escola de comércio
- Encontrar um médico próximo
- Receber uma solicitação de amizade de um perfil duplicado de alguém que você conhece

Links e recursos

aka.ms/edu-cybersecurity-guide

aka.ms/edu-cybersecurity

aka.ms/what-is-phishing

aka.ms/what-is-malware

aka.ms/parental-control-apps