

## INICIANDO A CONSCIENTIZAÇÃO SOBRE SEGURANÇA CIBERNÉTICA

Seu filho está participando das aulas do Currículo Estudantil CyberSmart! que ajudará sua família a iniciar um diálogo sobre segurança cibernética. A abordagem do CyberSmart! é baseada em pesquisa, concentrando-se nas melhores práticas da indústria de segurança cibernética.

CyberSmart! acredita que os alunos necessitam utilizar a Internet com segurança para aprendizagem, interação social e preparação para a universidade e trabalho no século 21 e cidadania.

Filtreadores de segurança, software anti-spam e outras soluções tecnológicas são úteis, mas não são suficientes, para manter as crianças e adolescentes protegidos. Na verdade, a segurança na Internet depende das decisões que os jovens tomam quando estabelecem, mantêm e utilizam computadores e a Internet. É por isso que CyberSmart! ensina habilidades de pensamento crítico e tomada de decisão.

### Segue abaixo o que ensinamos sobre segurança cibernética de acordo com a idade do aluno:

- Todos os computadores conectados à Internet estão vulneráveis a ataques – em casa, na escola, no trabalho e na biblioteca. Não importa o tipo de ataque – vírus, Trojan, fraude eletrônico, corrupção da rede ou qualquer outro – há maneiras do utilizador evitá-los.
- Muitos dos jovens sabem mais sobre computação do que seus pais, portanto, eles têm a responsabilidade de ajudar a sua família a desenvolver boas práticas de segurança cibernética.
- Crianças, adolescentes e adultos são vítimas de roubo de identidade. Estes furtadores de identidade coletam, roubam e utilizam informação privada, tais como número do seguro social, para fazer de conta que são essas pessoas e obterem carteira de motorista ou cartões de crédito no nome da pessoa roubada.
- A informação privada de identidade inclui nome completo da pessoa, endereço para correspondência, e-mail, número de telefone, número de cartões de crédito e número do seguro social.
- Senhas podem acabar em mãos erradas quando o aluno as compartilha voluntariamente com seus amigos, quando pessoas que o aluno conhece conseguem adivinhá-las e quando são furtadas por criminosos profissionais.
- As senhas mais seguras são criadas da combinação de oito ou mais letras, números e símbolos. Não deve ser utilizada nenhuma informação privada que possa ser adivinhada facilmente ou palavras do dicionário.
- Não abra e-mails ou aceite mensagens instantâneas de pessoas que não conhece. Não responda spam; nunca

## O que é segurança cibernética e por que é importante?

A aprendizagem sobre questões de segurança cibernética pode fazer com que a sua família se sinta mais protegida e segura on-line. A segurança cibernética é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares.

### Segue abaixo o que a família pode fazer:

- Fale com os seus filhos sobre o que fazem on-line. Informe aos seus filhos que você entende a importância do uso da Internet e outros meios de comunicação, tais como celular, nas suas vidas.
- Informe ao seu filho que as dificuldades com segurança, tais como a proteção de identidade dos membros da família, proteção de informação armazenada nos computadores e prevenção de interferências nos computadores e redes de comunicação são uma responsabilidade compartilhada por todos os membros da família.
- Revise as normas de segurança de senha com sua família. Certifique-se que você saiba todas as senhas de seus filhos mais jovens e que todos os membros da família seguem as regras de criação de senhas seguras, protegendo-as e mudando-as no mínimo a cada seis meses.
- Converse sobre os riscos associados a ofertas tentadoras on-line, tais como fazer download gratuitamente, compartilhar arquivos, mensagens de como adquirir dinheiro rapidamente, brindes e cartas-correntes. Converse sobre formas de como lidar com estas situações.
- Faça com que a família inteira participe da criação de um plano de segurança cibernética atualizando-o duas vezes por ano, incluindo a instalação de firewalls, software de segurança atualizados, proteção de redes de comunicação sem fio e fazendo backup de informação regularmente.
- Se você acha que sua família foi vítima de roubo de identidade ou fraude on-line, entre