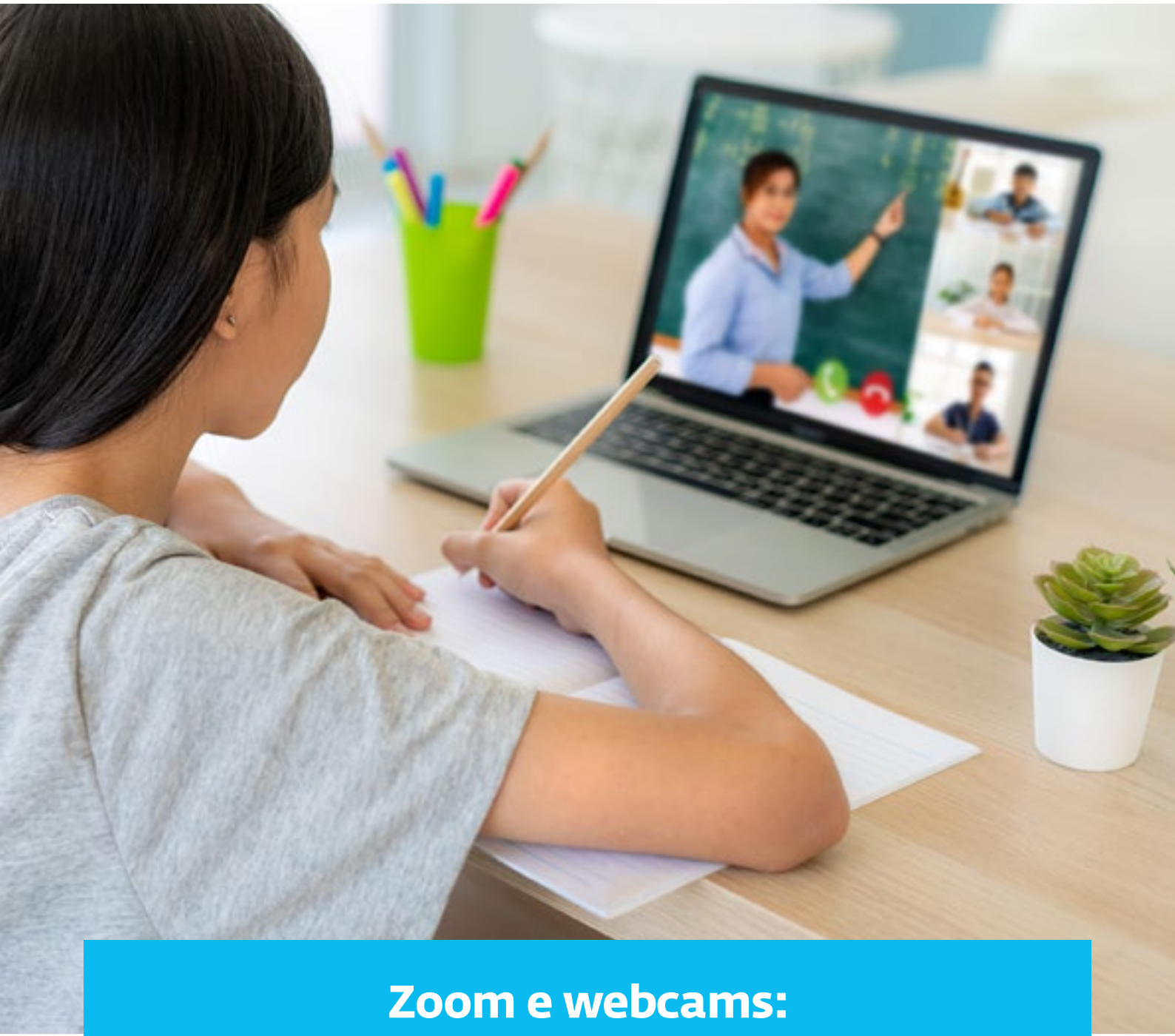
Digipais

UMA INICIATIVA DA saferkidsonline by eset



Zoom e webcams:
como proteger a privacidade dos pequenos

O Zoom, Meet, Teams e outros aplicativos similares são tendência há muitos anos, mas depois de 2020 a maioria das crianças (e dos pais) teve que se adaptar repentinamente a uma nova realidade onde as vídeo-chamadas são parte do dia a dia. Por isso, tornou-se mais importante do que nunca cuidar tanto de nossa cibersegurança como das crianças.

Uma das mudanças mais drásticas trazidas pela pandemia foi sem dúvidas a passagem abrupta para o virtual na maioria das áreas da vida: o trabalho, o colégio, atividades recreativas e mais. Em 2021, ainda se está tentando definir o que fazer com tudo isso enquanto se estabelece uma nova normalidade.

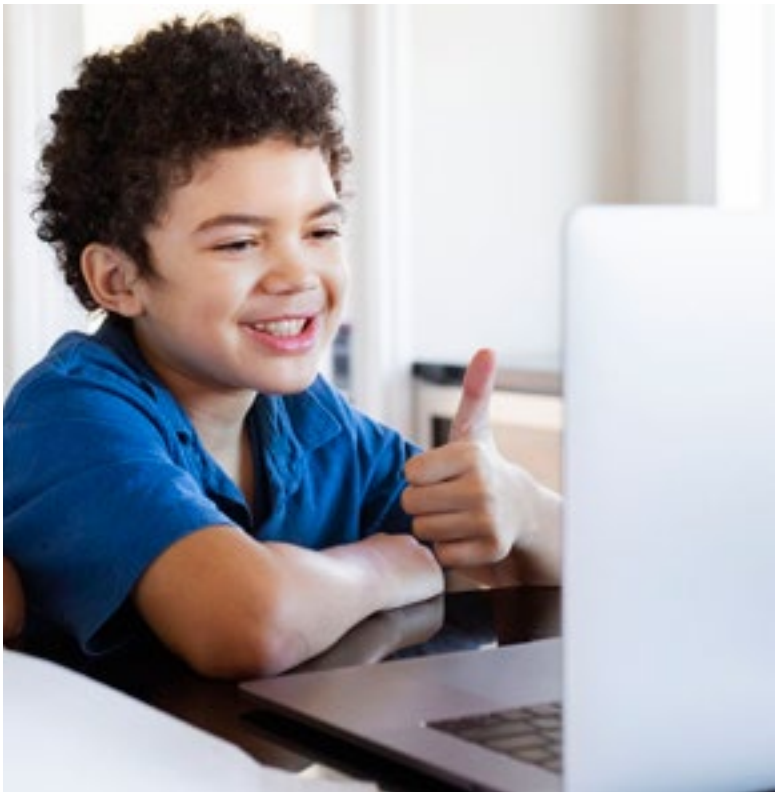
Como sabemos que essas mudanças podem ser assustadoras, nós da ESET queremos lembrar a todos os digipais alguns conselhos para cuidar da segurança das crianças ao utilizar dispositivos eletrônicos e o aplicativo Zoom para assistir a suas aulas ou outras atividades.

Cobrir a webcam quando não for utilizar

Utilizando códigos maliciosos, **os cibecriminosos podem tentar comprometer um dispositivo, obtendo acesso a sua câmera ou microfone sem o consentimento das vítimas, espiando os aspectos mais íntimos de suas vidas (spyware).** As motivações variam: alguns acham emocionante a ideia de ver alguém em segredo, outros buscam extorquir suas vítimas ameaçando com publicações desses vídeos se não receberem dinheiro.

Nossas recomendações para proteger as crianças dessa ameaça são:

- Ensinar às crianças a cobrir suas câmeras sempre que não estejam sendo usadas;
- Garantir que a configuração padrão da webcam seja sempre "desligada";
- Utilizar soluções de segurança capazes de proteger as câmeras em nível de software;
- Educar as crianças para que não façam nada em frente a uma webcam descoberta que não fariam se tivesse alguém olhando;
- Dar o exemplo: cobrir as câmeras de toda a família.



Configurar a segurança da plataforma de vídeo-chamadas usada

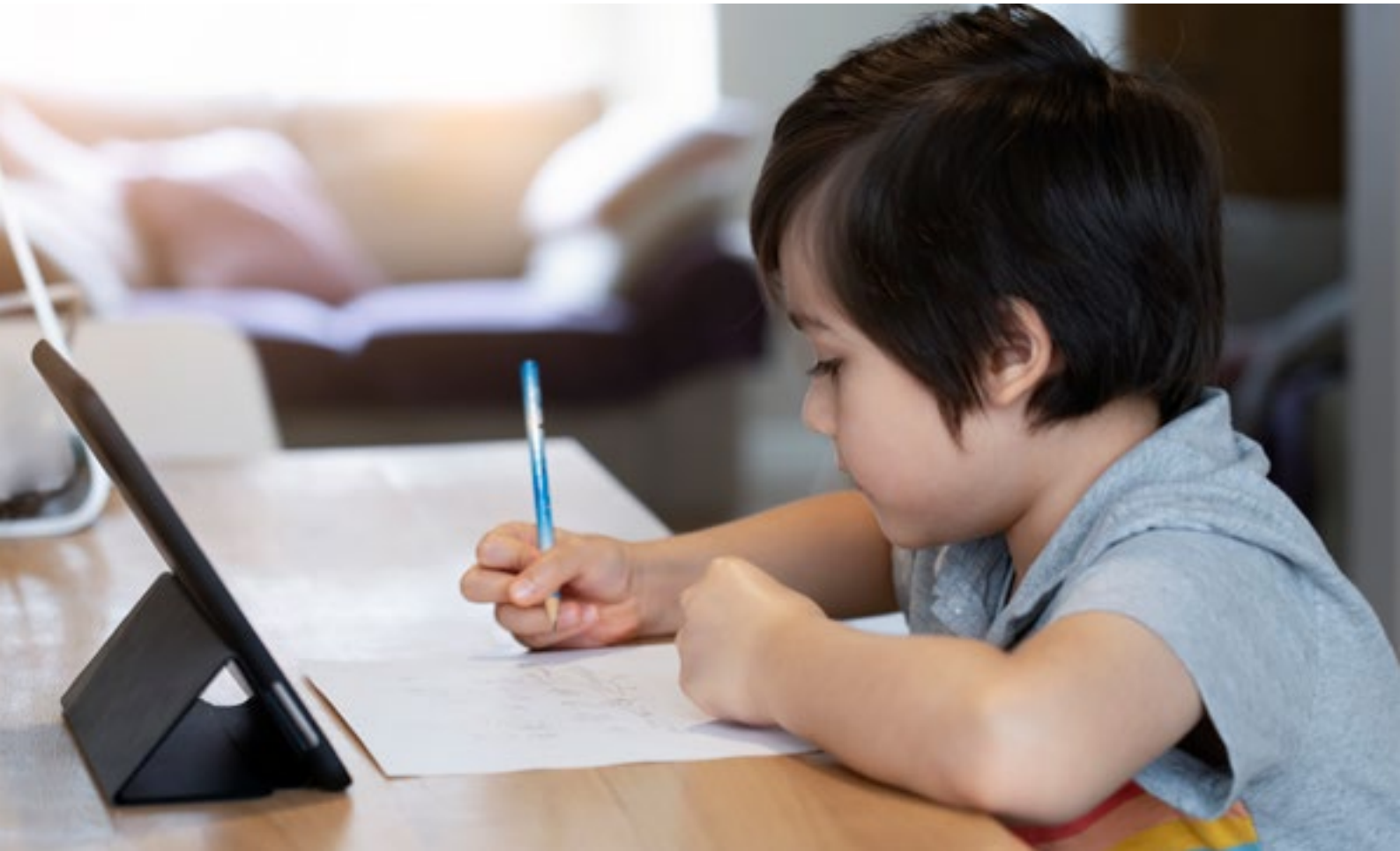
Como já dissemos, a mudança para o virtual afetou a todos nós e **as plataformas de vídeochamadas não estiveram isentas de sofrer violações de cibersegurança, hackeamentos, filtragem de dados, entre outros.** Por isso é importante configurá-las desde casa para tentar eduzir ao máximo os riscos de ficar envolvido nesses ataques.

» Garantir que as chamadas sejam privadas e que só possam ser acessadas com senha u link para evitar intrusos nelas.
» Iniciar as reuniões sempre com a câmera desligada e, se for obrigatório, ligá-las ssegurando que o fundo seja mudado, para que esteja embaçado ou usando um fundo predeterminado do Zoom para evitar revelar informações pessoais involuntariamente.
» Educar as crianças para que não compartilhem (nem por escrito, nem por conversa) informações pessoais ou confidenciais.
» Ativar o duplo fator de autenticação (2FA). O Zoom adicionou essa possibilidade no final de 2020 e é sempre uma grande forma de adicionar uma camada de segurança às vídeo-chamadas.

Baixar os aplicativos oficiais e sempre atualizá-los

Os aplicativos de mensagem, vídeo-chamadas ou até jogos, devem ser sempre baixados a partir da loja oficial do celular ou do PC ou notebook. Se baixados em sites não oficiais, pode acontecer que sejam aplicativos falsos ou com malware que infecte os dispositivos.

Após baixá-los, é importante atualizá-los apenas se lançada uma nova versão. Isso ocorre para que com cada atualização sejam reparadas vulnerabilidades com patches ou porque surgem novas fun-



ções ou camadas de segurança que se tornam importante incorporar em nossos dispositivos para evitar ataques.

Usar soluções de controle parental para proteger nossos filhos enquanto eles se divertem

Após as aulas, sejam virtuais ou presenciais, é muito provável que as crianças queiram, em algum momento, usar os dispositivos eletrônicos para jogar, publicar nas redes sociais ou simplesmente para se distrair. Isso é algo comum nos nossos dias e acontece cada vez com mais frequência. **Por isso, é importante, além de educá-los sobre cibersegurança, contar com uma solução de segurança com Controle Parental como o ESET Parental Control para Android.** Esta solução evita ataques de cibercriminosos, bloqueia sites inapropriados para crianças, desliga os dispositivos automaticamente após um tempo determinado de uso, entre outras funções-chave para evitar que as crianças passem por situações desagradáveis.

Com estas recomendações, já estamos prontos para que nossas crianças participem das aulas, joguem e falem com seus amigos de forma segura!

Queremos mais **Digipais** para capacitar as crianças e ensiná-los a navegar com segurança.

Você está pronto para se juntar a nós neste desafio?

www.digipais.com.br