****

**Afstandsonderwijs: de beveiligingsuitdaging**

*Sophos' tips eenvoudig samengevat in een eenvoudige gids voor ouders en studenten*

**8 februari 2021** – In het secundair onderwijs start vandaag de ‘afkoelingsperiode’. Die duurt tot 12 februari, waarbij de meer dan 1.000 middelbare scholen in Vlaanderen dicht blijven en de leerlingen voltijds afstandsonderwijs krijgen.

Het is dan ook het uitgelezen moment voor de cybersecurity-experts van Sophos om het belang van cyberveiligheid nogmaals onder de aandacht te brengen en jongeren te beschermen tegen eventuele gevaren en onaangename gevolgen van bepaalde veiligheidsrisico’s.

Het toepassen van effectieve technologische oplossingen blijft een essentiële voorwaarde voor degenen die thuis studeren: het is altijd nodig om te controleren of de apparaten up-to-date zijn en of er goede kwaliteitssoftware is geïnstalleerd, maar er zijn ook andere factoren die moeten worden geëvalueerd.

Hieronder enkele simpele maatregelen:

**Internettoegang**

Om het afstandsonderwijs te faciliteren, bieden veel leraren links naar online leermiddelen. Dit kunnen gratis video's zijn die worden gehost op sites van derden, zoals YouTube en Vimeo, materiaal op school of bronnen op externe sites, of die door de school zijn gekocht. Docenten kunnen ook activiteiten opzetten waarbij studenten hun eigen webgebaseerde onderzoek moeten doen. Al deze initiatieven vereisen dat kinderen toegang hebben tot internet. De uitdaging is om dit allemaal mogelijk te maken en hen tegelijkertijd te beschermen tegen ongepaste websites.

Sophos raadt aan om een ​​account voor kinderen aan te maken en vervolgens ouderlijk toezicht in het besturingssysteem in te schakelen om zo te kunnen beperken tot welke sites ze toegang hebben. Voor Windows 10-gebruikers is het voldoende om de gezinsopties in de zoekbalk te gebruiken en vanaf daar ouderlijk toezicht in te schakelen. Beperkt surfen op het web op Microsoft Edge wordt dan automatisch ingeschakeld terwijl privé (incognito) surfen op het web is uitgeschakeld. Degenen die een Mac gebruiken kunnen dan weer kiezen tussen verschillende modi, afhankelijk van de gebruikte versie.

Sophos stelt daarnaast ook het gebruik van een antivirusproduct voor thuisgebruik voor. Liefst eentje dat webfiltering voor ouders bevat, zodat die controle hebben waartoe kinderen en tieners vanaf hun computer toegang hebben.

**Gedeelde apparaten**

Veel studenten zullen in de huidige omstandigheden een gedeeld apparaat moeten gebruiken om toegang te krijgen tot schoolwerk. Misschien is dit wel de gezinslaptop of -tablet die ook door hun broers en zussen wordt gebruikt.

Het is essentieel om iedereen een gebruikersaccount op het gedeelde apparaat toe te wijzen.

Hiermee kunt u ouderlijk toezicht instellen zonder dat dit de ouderlijke toegang tot het apparaat beïnvloedt. Bovendien helpt deze waarschuwing kinderen ook om goede beveiligingsgewoonten te verwerven, zoals het hebben van hun eigen wachtwoord (hoewel ze dit, afhankelijk van hun leeftijd, met hun ouders moeten delen).

**Het wachtwoord**

Bij het volgen van afstandsonderwijs is het vaak de eerste keer dat kinderen en tieners wachtwoorden moeten beheren. Ze hebben waarschijnlijk een wachtwoord voor school-e-mail en online leermiddelen, en als ze een aparte account op een gedeeld apparaat hebben, hebben ze daar ook een wachtwoord voor.

Sommige wachtwoorden, zoals die voor onlinebronnen die door de school zijn toegewezen, zijn door de school zelf ingesteld en het is mogelijk dat u ze niet kunt wijzigen. Maar in die gevallen waarin u de inloggegevens wel kunt wijzigen om toegang te krijgen tot sites, online platforms enz. is het belangrijk om dit meteen te doen. Met behoud van de standaardwachtwoorden weet u niet zeker hoeveel andere accounts zijn geconfigureerd met hetzelfde wachtwoord of hoeveel andere mensen toegang hebben tot de lijst met gekozen standaardinstellingen.

Het maken van moeilijk te kraken wachtwoorden is een taak die kinderen alleen kunnen doen en het is een geweldige kans om ze kennis te laten maken met zogenaamde wachtwoordzinnen: het advies is om te beginnen met woorden die hun interesses weerspiegelen, zodat zinnen gemakkelijker te onthouden zijn, en werk vervolgens met hen samen om ze complexer te maken.

Het kan natuurlijk gebeuren dat kinderen wachtwoorden vergeten, dus om te voorkomen dat ze elke maandagochtend opnieuw moeten worden ingesteld, adviseren Sophos-experts om een ​​wachtwoordbeheerder te gebruiken, een tool die ook uitermate handig is voor volwassenen die vaak over tientallen wachtwoorden beschikken.

In deze specifieke context kan het echter gemakkelijker en praktischer zijn om ergens wachtwoorden te schrijven, maar het is belangrijk om ze op een veilige plaats te bewaren ... dus zeker en vast geen Post-it op uw pc-monitor!

**Leerzame apps**

Thuisonderwijs vereist vaak het downloaden van nieuwe apps, zowel educatieve als die om studenten online te laten werken.

Welke apps u ook moet downloaden en gebruiken, het is van cruciaal belang om alleen op officiële app-winkels te vertrouwen. Het kan ook handig zijn om de meningen en ervaringen van andere mensen over nieuwe apps te lezen om ze te downloaden en er zeker van te zijn dat ze geen valstrikken verbergen zoals fleeceware, verraderlijke programma's die geld stelen na een "gratis" proefperiode.

In dit verband waarschuwt Sophos voor recensies en sterbeoordelingen in de app-winkels zelf: het is niet mogelijk om de bron te verifiëren en ze kunnen worden gedeeld door degenen die de app nog niet hebben gebruikt, aangezien positieve beoordelingen en recensies online voor een paar cent kunnen worden gekocht. Het is daarom beter om reviews te zoeken in de vorm van onafhankelijke gebruikers of in de discussies van onlinecybersecuritygroepen.

**Privacy**

Afstandsonderwijs is ook een uitstekende gelegenheid om met jongeren over digitale privacy te praten. Er zijn verschillende stappen die u moet nemen om u online te beschermen, waaronder:

• Controleer de autoriteitssettings in uw browser. Zorg ervoor dat uw locatie, camera, microfoon en meldingen zijn ingesteld op 'Vragen voordat u toegang verleent'

• Stel privacy-opties in op iOS- en Android-apparaten.

• Wees voorzichtig als de camera is ingeschakeld, controleer wat er zichtbaar is als de webcam actief is. Verleen apps of websites standaard geen toegang tot uw camera of webcam

Sleutelwoorden als het om privacy gaat zijn kennis en bewustwording. Het is belangrijk om jongeren het belang van privacy te laten inzien: zorgvuldig kiezen wat ze delen, hoe en met wie. Er is een enorm verschil tussen de docent een link naar een video op een persoonlijke schijf geven of deze naar YouTube uploaden voor openbare weergave.

**Thuis wifi**

Het is de moeite waard om even de tijd te nemen om te controleren of uw wifi-thuisnetwerk veilig is, zowel om uw persoonlijke gegevens te beschermen als om uw bedrijfsnetwerk te beschermen.

Zodra een aanvaller voet aan de grond heeft op een apparaat binnen het thuisnetwerk, kan hij gemakkelijk snuffelen over wat er gebeurt in het digitale leven van zijn bewoners. Net zoals het voor hem gemakkelijk wordt om toegang te krijgen tot andere apparaten, inclusief persoonlijke of zakelijke pc's en van daaruit misschien zelfs toegang tot het bedrijfsnetwerk.

**Het belang van proactiviteit**

Het managen van het afstandsonderwijs is, naast andere dagelijkse verplichtingen, een grote uitdaging voor gezinnen en het kan moeilijk zijn om de tijd en energie te vinden om zich ook op het veiligheidsaspect te concentreren.

Het is echter belangrijk om daar tijd voor te vinden, misschien in het weekend, wanneer u het minder druk heeft. Houd er rekening mee dat veel van de te nemen controles en voorzorgsmaatregelen slechts één keer hoeven te worden aangepakt en ingesteld.

**Over Sophos**

Als een wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties, ongeacht bedrijfsgrootte, in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen van vandaag. Aangedreven door SophosLabs, een wereldwijd team gespecialiseerd in bedreiginginformatie en wetenschappelijke data, beveiligen Sophos’ cloud-native en AI-verbeterde oplossingen endpoints (laptops, servers en mobiele apparaten) en netwerken tegen immer evoluerende cybercriminele tactieken en technieken. Hieronder vallen onder meer geautomatiseerde en actieve, vijandige inbreuken, ransomware, malware, exploits, data-exfiltration, phishing en meer. Het cloudgebaseerde Sophos Central-platform integreert Sophos’ gehele portfolio - van Intercept X-endpointoplossing tot XG Firewall - in een enkel systeem: Synchronized Security.

Sophos-producten zijn exclusief verkrijgbaar via een wereldwijd kanaal van meer dan 53.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën ook beschikbaar aan consumenten via Sophos Home. Het bedrijf is gevestigd in Oxford, Verenigd Koninkrijk. Meer informatie: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Sandra Van Hauwaert, Square Egg Communications, sandra@square-egg.be, GSM 0497251816.