HANDIGE CHECKLIST OM CYBERAANVALLEN TE VOORKOMEN

Het is nooit helemaal uit te sluiten dat je te maken krijgt met cybercriminaliteit. Wel kun je proberen de kans zo veel mogelijk te verkleinen. Met de volgende 8 tips houd je jouw school veilig. Hoeveel kun jij er afvinken van deze checklist?

- ☐ **Gebruik antivirussoftware**. Zorg ervoor dat alle laptops en andere apparaten van docenten en leerlingen worden beschermd door antivirussoftware om te voorkomen dat ze per ongeluk malware downloaden.

- ☐ **Gebruik een wachtwoord policy**. Laat docenten en leerlingen eens in de drie maanden hun wachtwoord wijzigen. Stel bepaalde eisen aan hoe een wachtwoord opgebouwd moet zijn. En nee, een verandering van "superman09" naar "superman10" moet je niet goed willen keuren ☺

- ☐ **Negeer nooit software updates.** Updates zijn onder andere bedoeld om jou en de school veilig te houden. Controleer of de software op laptops, digiborden en andere apparaten van docenten en leerlingen up-to-date is en schakel automatische updates in.

- ☐ **Vergrendel apparaten altijd als je ze niet gebruikt**. Zo voorkom je ongewenste toegang. Dit geldt voor laptops, maar ook bijvoorbeeld voor de digiborden in de klas. Die kunnen eenvoudig vergrendeld worden met een NCF kaartlezer of vingerafdrukscanner.

- ☐ **Zorg voor een veilige internetverbinding**. Naast leerlingen en docenten maken ook apparaten steeds vaker gebruik van het internet. Slimme apparaten maken automatisch verbinding om gegevens uit te wisselen en dat vormt een risico. Zorg dat je netwerk veilig is en sta alleen internettoegang toe waar dit noodzakelijk is.

- ☐ **Controleer derde partijen grondig**. Zorg ervoor dat alle externe platformaanbieders en overige derde partijen waar je op school mee werkt, digitale veiligheid hoog in het vaandel hebben staan.

- ☐ **Monitor de systemen voortdurend**. Een hacker stopt niet aan het einde van een schooldag, in het weekend of in de schoolvakanties. Zorg dat je al je systemen voortdurend (laat) controleren en analyseren op ongewone activiteiten die kunnen wijzen op een aanval.

- ☐ **Zorg voor bewustwording**. Een veilige leeromgeving is niet alleen een verantwoordelijkheid van de ICT-beheerder en de directeur. Organiseer ook regelmatig sessies voor leerlingen en docenten, zodat iedereen op de hoogte is van de nieuwste cyberbedreigingen en trends.