**Onderwerp:** Terugkoppeling Beveiligingsincident BYOD-laptop

Beste [Naam collega],

Naar aanleiding van het beveiligingsincident dat zich heeft voorgedaan met uw BYOD-laptop, informeer ik u graag over de maatregelen die zijn genomen en de vervolgstappen die u dient te ondernemen.

**Analyse van het incident**

Het incident is veroorzaakt doordat er op een schadelijke link in een phishing-e-mail is geklikt. Hierdoor is uw laptop geïnfecteerd met malware, wat heeft geleid tot blokkering van uw apparaat en encryptie van bestanden op de gedeelde netwerkschijf.

**Maatregelen en oplossingen**

1. **Beveiliging en isolatie:**
   * Uw laptop is direct van het netwerk verwijderd om verdere verspreiding van de malware te voorkomen.
   * Het netwerk is gecontroleerd op andere mogelijke besmettingen.
2. **Herstel van de bestanden:**
   * Er wordt geprobeerd de bestanden van de gedeelde netwerkschijf te herstellen via back-ups.
3. **Herconfiguratie van uw laptop:**
   * Uw apparaat wordt volledig schoongemaakt en opnieuw geconfigureerd. Hierdoor zal u tijdelijk geen toegang hebben tot de laptop.
4. **Preventieve maatregelen:**
   * Er wordt extra training aangeboden om phishing-e-mails te herkennen.
   * Onze beveiligingsprocedures worden aangescherpt om toekomstige incidenten te voorkomen.

**Uw actiepunten**

* **Gebruik een tijdelijke werkomgeving:** U ontvangt binnenkort een vervangende laptop waarmee u kunt blijven werken.
* **Wees alert op phishing-e-mails:** Klik niet zomaar op links in e-mails, vooral als deze te mooi lijken om waar te zijn.

**Vervolg**

We blijven u op de hoogte houden van de voortgang met betrekking tot het herstel van uw bestanden en de beveiliging van uw laptop. Als u verdere vragen of zorgen heeft, kunt u altijd contact opnemen met de servicedesk via [contactgegevens].

Bedankt voor uw geduld en medewerking.

Met vriendelijke groet,  
[Uw naam]  
[Uw functie]  
[Organisatie]  
[Contactgegevens]