Beste ondernemers,

 U ontvangt deze mail omdat uit gesprekken met Parkmanagement Lage Weide blijkt dat er behoefte is aan voorlichting over cybercriminaliteit. We zien dat cybercriminaliteit sinds de ‘intelligente lockdown’ [sterk is toegenomen](https://insights.abnamro.nl/2020/06/meer-dreiging-cybercrime-door-corona-maar-perceptie-risico-lager/). En dat terwijl we juist nu extra afhankelijk zijn van onze online middelen. Om ondernemers zo goed mogelijk te kunnen ondersteunen op dit gebied willen we weten waar de specifieke behoeftes liggen en hoe het gesteld is met jullie digitale veiligheid. Op basis daarvan kunnen we dit najaar een gratis bijeenkomst/training op maat voor u ontwikkelen.

Om deze informatie op te halen nemen we vanuit het team Digitale Veiligheid van de gemeente Utrecht een vragenlijst af onder ondernemers. Tussen 20 juli en 23 juli loopt onze collega Coen Simons langs ondernemers op Lage Weide om de vragenlijst samen met u in te vullen. Hiervoor vragen wij u ongeveer vijf minuten van uw kostbare tijd. Wij begrijpen dat het COVID-19 virus moeilijke tijden met zich meebrengt, daarom zal hij het zo kort mogelijk houden.

Met de informatie uit de vragenlijst kunnen wij samen met ondernemers stappen zetten naar een veilig digitaal Utrechts ondernemersklimaat. De gegevens worden niet gepubliceerd en zullen niet te herleiden zijn tot uw organisatie.

Lukt het niet om de vragenlijst in te vullen met onze collega? Dan kunt u in de bijlage de vragenlijst vinden. Als u deze heeft ingevuld kunt u deze sturen naar coen.simons@utrecht.nl

Alvast dank voor uw moeite.

Met vriendelijke groet,

Team Digitale Veiligheid van de gemeente Utrecht

**Vragenlijst:**

**1. Gebruikt u digitale apparatuur/online middelen (website, mail, online bestellingen/facturering in uw bedrijf?**

………………………………………………………………………………

**2. Is uw bedrijf ooit slachtoffer geweest van cybercriminaliteit?**

A) geen pogingen gehad dus geen slachtoffer

B) Ja, slachtoffer

C) Ja poging ondervonden, maar geen slachtoffer

D) Weet niet

**3. Welke soort cybercrime heeft er plaatsgevonden?**

A) ongeautoriseerd gebruik van het bedrijfsnetwerk

B) Ransomware (computer geïnfecteerd met berichten dat je geld moet betalen)

C) Skimming (iemands betaalgegevens kopiëren)

D) Phishing (oplichting door persoon betaalgegevens te laten doorsturen)

E) Smaad/laster

F) Spionage

G) Fraude/oplichting

H) Afpersing

I) Ddos-aanval (systemen moeilijk bereikbaar maken)

J) Diefstal van data dragers (e.g. usb stick, externe harde schijf)

K) Identiteitsmisbruik

L) Chantage via het internet

M) Defacing

N) Diefstal van gegevens

O) Hacking (iemand die binnen treed in systemen)

P) Malware

**4.  Heeft uw organisatie maatregelen getroffen? (dit kan zijn: wachtwoorden met regelmaat wijzigen, regels opstellen voor online betalingen, geen mail van onbetrouwbare afzenders openen, back-ups, virusscanners, uitgeschreven plannen voor preventie of wat te doen als u slachtoffer bent, etc.)**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**5. Waar is uw bedrijf bereid toe?**

A) extra tijd investeren in digitale veiligheid

B) extra geld investeren in digitale veiligheid

C) extra middelen investeren in digitale veiligheid

D) Niets extra’s te investeren in digitale veiligheid

**6. Waar heeft uw bedrijf behoefte aan?**

A) gratis tools

B) betaalde tools

C) voorlichting over digitale veiligheid

D) live cursussen over digitale veiligheid

E) digitale cursussen over digitale veiligheid

F) bedrijf analyses over digitale veiligheid

G) penetratietest

H) expert gesprekken

I)   een online platform waar u met andere ondernemers over digitale veiligheid kan praten

Zijn er nog vragen?

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………