## **Bijlage 2.1 Sjabloon Gebruikersinstructie**

Naam: *Veilig wachtwoordbeleid: Hoe veilige wachtwoorden te creeren en beheren*

Doel of omschrijving: *Gebruikers instrueren over sterkere wachtwoorden*

Doelgroep: *Alle gebruikers*

Auteur: *Kevin Keen*

### Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Versie** | **Auteur** | **Aanpassing** |
| *8-02-2024* | 1.0 | Kevin Keen | Eerste versie |
|  |  |  |  |
|  |  |  |  |

**Inleiding:**  
Het gebruik van sterke, unieke wachtwoorden voor elke online service of account is cruciaal in de hedendaagse digitale wereld. Simpele of hergebruikte wachtwoorden kunnen leiden tot ernstige beveiligingsrisico's, waaronder het compromitteren van gevoelige informatie.

**Waarom Simpele Wachtwoorden een Slecht Idee Zijn:**  
Een kort verhaal toont het gevaar: Alex gebruikte "Zomer2023" voor al zijn accounts, wat resulteerde in een gehackte e-mail en blootstelling van gevoelige gegevens. Dit voorbeeld onderstreept het belang van het gebruik van sterke, unieke wachtwoorden.

**Hoe Maak je een Veilig Wachtwoord:**

**Lengte en Complexiteit:** Kies voor wachtwoorden van minimaal 12 tekens met een mix van hoofdletters, kleine letters, cijfers, en speciale tekens.

**Vermijd Voorspelbare Patronen:** Vermijd gemakkelijk te raden informatie zoals namen of geboortedata.

**Gebruik Wachtwoordzinnen:** Een effectieve methode is het gebruik van wachtwoordzinnen. Dit zijn lange zinnen of combinaties van woorden die makkelijk te onthouden zijn maar moeilijk te raden voor anderen.

**Onthouden van Wachtwoorden met Geheugensteuntjes:**

In plaats van wachtwoordbeheerders kun je ook geheugensteuntjes gebruiken om complexe wachtwoorden te onthouden. Bijvoorbeeld, het wachtwoord "IkW@8elkDag30Min!" kan herleid worden uit de zin "Ik Wandelt elke Dag 30 Minuten!" Dit maakt het wachtwoord niet alleen sterk en uniek, maar ook makkelijk te onthouden door het persoonlijke geheugensteuntje.

**Conclusie:**  
Sterke, unieke wachtwoorden zijn essentieel voor het beschermen van je online identiteit en gevoelige informatie. Door het volgen van onze richtlijnen en het investeren in goede wachtwoordgewoonten, zoals het gebruik van geheugensteuntjes, bescherm je effectief jezelf en je organisatie tegen digitale bedreigingen.