HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

HACKING

Wat is hacking?

Hacking is het digitaal binnentreden van computers of systemen zonder toestemming.

Hoe gebeurt het?

Meestal gebeurt dit door het stelen van inloggegevens, zoals wachtwoorden. Het is altijd strafbaar als dit gebeurt zonder toestemming van de eigenaar van die gegevens.

Wat is het doel?

Het doel is meestal om gevoelige informatie te verzamelen, maar het kan ook worden ingezet om bijvoorbeeld het slachtoffer af te persen.

Welke methodes zijn er?

- Door te hengelen naar inloggegevens via slimme trucs → phishing
- Het achterhalen van iemands inloggegevens door te raden of slimme vragen te stellen aan het slachtoffer → social engineering
- Door iemand te dwingen zijn gegevens te vertellen → afpersing
- Door het slachtoffer malafide software te laten installeren → malware
- Het achterhalen van iemands inloggegevens via een datalek

REPRESSIE

Wat je vooral wel moet doen.

Stap 1

Verander direct de wachtwoorden van al je accounts met hetzelfde wachtwoord of een wachtwoord dat er op lijkt. Hetzelfde wachtwoord voor meerdere accounts gebruiken is niet veilig!

Stap 2

Stel voor belangrijke accounts 'tweestapsverificatie' in via accountinstellingen. De crimineel kan dan niet meer met enkel het wachtwoord binnentreden. Meer uitleg over hoe je dit per account doet, vind je (in het Engels) via Authy.com

Stap 3

Ga na welke informatie een kwaadwillende heeft kunnen stelen via het betreffende account. Neem passende maatregelen op basis van welke informatie gestolen is. Heeft men bijvoorbeeld toegang verkregen tot je bankgegevens? Maak dan melding bij je bank en politie.

Stap 4

Zoek op wat de aanbieder van je account zelf adviseert bij een hack.

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

Stap 5

Scan je computer voor malware of virussen (bijvoorbeeld met malwarebytes).

Stap 6

Check via haveibeenpwned.com of er nog meer gegevens van je gelekt en gepubliceerd zijn.

Stap 7

Neem preventieve maatregelen om je wachtwoorden te beschermen.

PREVENTIE

Installeer een antivirusprogramma

Laat het antivirusprogramma geregeld je apparaten scannen op infecties. Schakel een eventueel meegeleverde firewall altijd in.

Gebruik lange wachtwoorden

Gebruik 12 tekens of meer en voor elke dienst een uniek wachtwoord. Waar mogelijk gebruik twee-stapsverificatie om je account te beschermen.

Installeer direct de software updates

Maak waar mogelijk gebruik van automatische updates. Installeer in andere gevallen zelf direct updates als deze beschikbaar zijn.

Maak alleen verbinding met vertrouwde wifi-netwerken

Bij openbare en onbeveiligde wifi netwerken kunnen anderen mogelijk zien wat je op het internet doet en welke gegevens je verstuurt. Verstuur dus geen gevoelige informatie en doe geen bankzaken.

Open geen berichten of onbekende bestanden die je niet verwacht of vertrouwt

Gebruik altijd je gezond verstand en ga hier niet op in, zelfs niet wanneer je de afzender kent.

Controleer het adres van websites

Is er geen hangslotje aan de linkerkant van de adresbalk? Vul dan geen gevoelige informatie in op de website.

Maak regelmatig back-ups

Door regelmatig back-ups te maken van bestanden of foto's, kun je schade van bijvoorbeeld gijzelsoftware of virussen beperken.