VNO-NCW West - Webinar Cyber Security – 29 mei 2020

Vragen en antwoorden aan Mimoent Haddouti , spreker Rabobank

1. Heeft de stijging van het misbruik ook te maken met betaalpassen etc en alleen via Rabobank?
   Dit betreft interne informatie die niet deelbaar is.

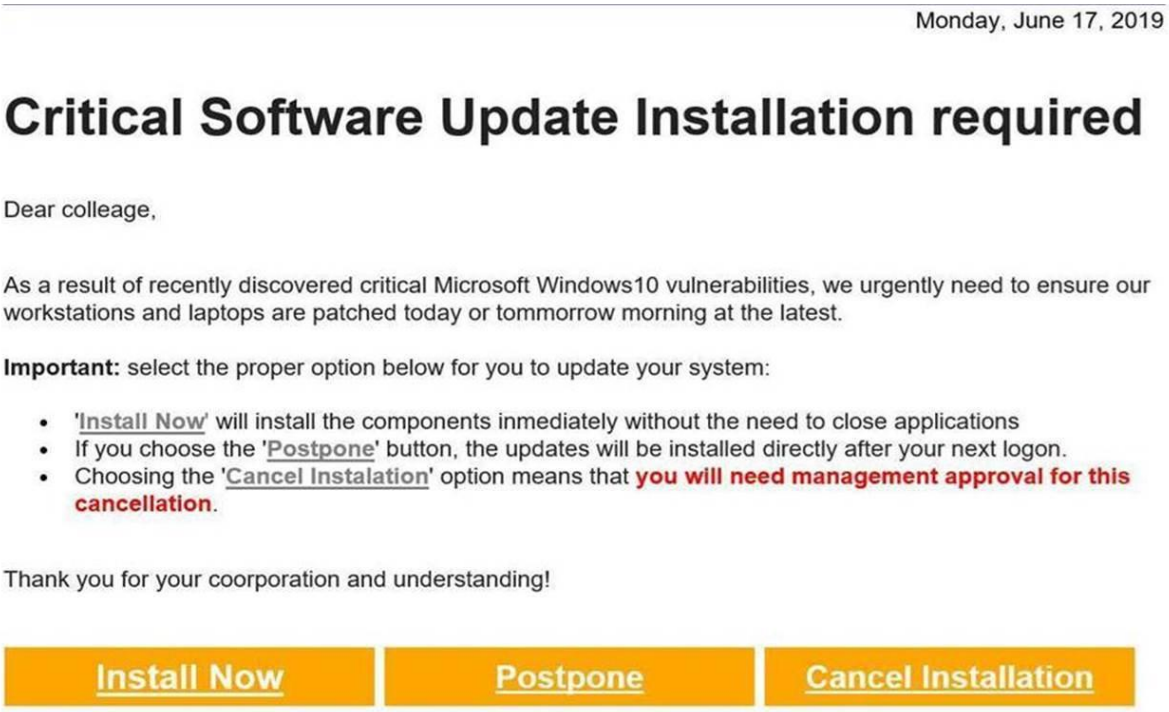
2. Hoe maken websites precies misbruik van Coco's-19?
   Op drie manieren:1) jouw aantrekken zodat de website eigenaar geld krijgt omdat de homepage vol staat met reclame (erg onschuldig) en 2) bedoelt om phishing te doen zodat je bijvoorbeeld aanvullende info aanvraagt en je persoonlijke gegevens achter laat, of 3) De website wordt gebruikt om mail vanaf te sturen (komt vertrouwd over) om jou te verleiden om een kwaadaardig linkje te klikken.

3. Rabo heeft 30k personeel over 39 landen thuiswerken, hoeveel man werken er tegelijk op het netwerk op jullie piek moment? (en is er nog een onderscheid tussen personeel wat wel of niet online mag?)
   In de afgelopen maanden hebben steeds rond >90% van alle medewerkers wereldwijd thuis gewerkt.

4. Op welk percentage ben je volwassen m.b.t. phishing tests?
   Er wordt een zogenaamd 'Tiered' aanpak gekozen. Bij deze aanpak wordt zichtbaar hoe medewerkers geleidelijk kennis op doen, en wennen aan Phishing e-mails die in de loop van de tijd steeds complexer worden en moeilijker te herkennen worden. Zo is een 'Tier 1' phishing e-mail voor een medewerker redelijk gemakkelijk te identificeren is. 'Tier 5' is het aller moeilijkst te herkennen en vergt dan ook training, zoals we die binnen Rabobank hebben opgezet.
   Rabobank heeft zich ten doel gesteld het percentage mensen dat niet afdoende in staat is een Phishing mail te herkennen naar een zo laag mogelijk percentage te brengen. 3% a 4% is een streefgetal, maar met een oplopende moeilijkheidsgraad (tier 1 / 5) zal dat percentage niet altijd gehaald worden.

	Easy to Detect				Difficult to Detect
Tier	1	2	3	4	5
Description	Easy to spot with basic knowledge	Slightly more difficult to spot, but with basic knowledge	Harder to spot, requires intermediate training and knowledge	Not so easy to spot, requires consistent training and knowledge	Difficult to spot, requires in depth knowledge and behaviour
Example	Multiple spelling errors, non-personal addressment, unprofessional look-and-feel, clicking a link will lead to a teachable moment	Little spelling errors, non-personal addressment, semi-professional look-and-feel, opening a file or clicking a link will lead to a teachable moment	No spelling errors, personalized, professional look-an-feel, opening a link or file and leaving credentials will lead to a teachable moment	Good spelling and language, highly personalized, professional look-an-feel, tricks used to mislead the addressee. Opening a file or clicking a link will lead to a teachable moment	Very professional level which is comparable to real phishing mails.

5. Hebben jullie een voorbeeld van een mailbericht voor de bewustwording?
   Zie hieronder:



Monday, June 17, 2019

Critical Software Update Installation required

Dear colleage,

As a result of recently discovered critical Microsoft Windows10 vulnerabilities, we urgently need to ensure our workstations and laptops are patched today or tommorrow morning at the latest.

Important: select the proper option below for you to update your system:

- 'Install Now' will install the components inmediately without the need to close applications
- If you choose the 'Postpone' button, the updates will be installed directly after your next logon.
- Choosing the 'Cancel Instalation' option means that **you will need management approval for this cancellation**.

Thank you for your coorporation and understanding!

Install Now | Postpone | Cancel Installation

6. Aansluitend: kunnen/willen jullie die kennis ook breed delen met het MKB?
   Daar zijn wij zeker toe bereidt. Daarvoor proberen we zoveel mogelijk aan te sluiten bij initiatieven waarbij MKB ook is aangesloten