

Task 1

Investigar E-mails



Introdução

Serão apresentados 7 e-mails conforme o [documento](#) estabelecido pela ANZ, e o objetivo é definir qual é malicioso e o porquê, tudo de acordo com minha análise e entendimento da área de segurança cibernética.

Task 1

Investigar E-mails



E-mail 1

← [Calendar] [Trash] [Envelope] [More]

FYI [Yellow Arrow] **Inbox** ☆

Adam John 10:25 am
Hey mate, Did you see all those new trailers from Games Con??

Velma Khan 10:27 am
to me ▾

Yeah just saw the trailer for ksp2. Dude it looks sick as!!!!

You gonna buy the preorder?

[Hide quoted text](#)

On Wed, 21 Aug. 2019, 10:26
<Adamm.johnnn1996@gmail.com> wrote:
Hey mate,
Did you see all those new trailers from Games Con??

Seguro

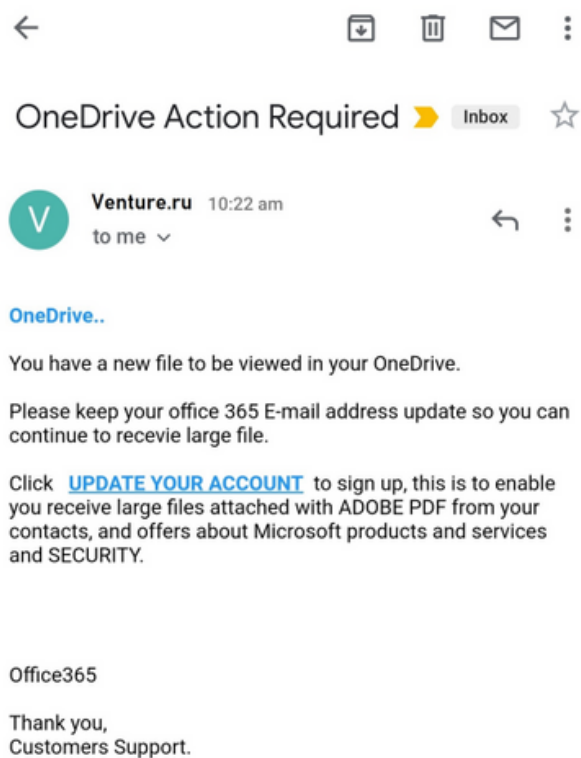
- Não apresenta links e domínios suspeitos.
- Pode-se concluir que é apenas uma conversa entre dois colegas de trabalho.
- O e-mail do remetente é gmail.com.
- Nenhuma abordagem comercial ou ameaçadora.

Task 1

Investigar E-mails



E-mail 2



Malicioso

- Domínio Russo
- Solicita o usuário a clicar no Hiperlink.
- E-mail genérico, sem marcação ao usuário e texto pouco elaborado.
- Ocasionalmente um SPAM.
- Não possui uma assinatura da Microsoft no rodapé.
- O e-mail tenta abordar uma curiosidade e urgência do usuário.

Task 1

Investigar E-mails



E-mail 3



Malicioso

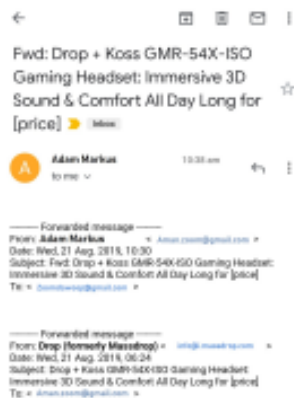
- Abordagem intimidadora e de urgência.
- link com a letra B errada.
- E-mail genérico, sem marcação ao usuário e texto pouco elaborado.
- Ocasionalmente um SPAM.
- Não possui uma assinatura do Facebook no rodapé.

Task 1

Investigar E-mails



E-mail 4



Pairing a closed-back design with custom-engineered acoustics, the Drop + Koss GMR-54X-ISO gaming headset offers truly immersive 3D sound—when gaming or listening to music. Crafted in a subtle midnight blue colorway, the headset features a lightweight headband for comfort during long sessions. It also comes with a splitter and a boom mic with a new adjustments.



Seguro

- E-mail comercial.
- E-mail bem elaborado.
- SPAM.
- Assinatura no rodapé.
- domínio gmail.
- Email empresarial.



Task 1

Investigar E-mails



E-mail 5

You are needed  Inbox 

 **Vincent** 11:25 am
to me 

Hi, my name is Vincent and I'm an FBI agent undercover in Uganda.

My W.A.E. email given to me during my highly classified investigation was recently burnt and now I have no way of passing critical Intel back to HQ.

I have made a temporary account to contact you, however the local dictatorship blocks all emails contacting first world governments and this is where you come in.

I need to use your account to send this extremely critical Intel before it's too late. This will require me accessing your email for security reasons.

Thank you in advance for your understanding.

Superintendent Vincent
FBI

Malicioso

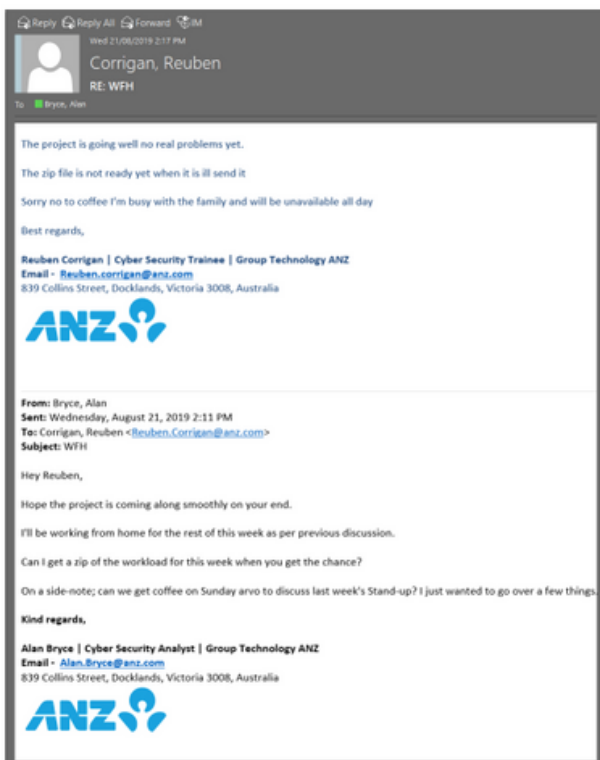
- Abordagem absurda, intimidadora e de urgência.
- Solicita dados pessoais do usuário.
- E-mail genérico, sem marcação ao usuário e o texto é fantasioso.
- Ocasionalmente um SPAM.
- Não possui uma assinatura do Facebook no rodapé.

Task 1

Investigar E-mails



E-mail 6



Seguro

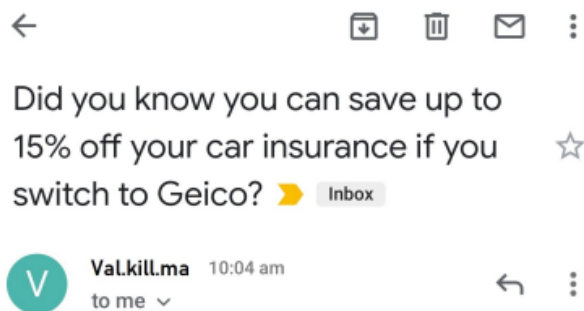
- Dento do domínio da empresa ANZ.
- Assinatura Eletrônica, para mostrar autenticidade.
- Conversa empresarial.

Task 1

Investigar E-mails



E-mail 6



Malicioso

- Email sem elaboração.
- Link suspeito.
- Link php, pode ser um shell malicioso.
- Abordagem de urgência.

hxxp://iwhrhwicy.urlif.y/receipt.php

Cheers,

Mike Ferris