SEGURANÇA DA INFORMAÇÃO

Webinar BYOD – *Bring Your Own Device*

AP2SI

metared PORTUGAL

AP2SI

A Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) é uma instituição sem fins lucrativos, fundada em Janeiro de 2012 e que tem como objetivo a promoção e divulgação do tema da segurança da informação e suas vertentes na sociedade portuguesa.

A nossa missão é contribuir para o desenvolvimento da Segurança da Informação em Portugal, de forma activa, através da sensibilização da sociedade, do desenvolvimento e promoção de orientações e da qualificação de indivíduos e organizações.

ap2si.org

geral@ap2si.org


BRING YOUR OWN DEVICE

O que é o BYOD?

- BYOD é o acrónimo de *Bring You Own Device* e representa uma prática em que uma organização permite aos seus utilizadores a utilização dos seus dispositivos para realizar o seu trabalho, ligando-os às redes e sistemas da organização, acedendo aos seus dados.

Vantagens do BYOD

- A principal vantagem do BYOD é a redução de custos para as organizações.
- Para os utilizadores é também confortável não duplicar a quantidade de dispositivos que têm a seu cargo

Alguns dados sobre BYOD

- +240 horas/ano ganhas pelas organizações
- ~79% das organizações nos EUA adoptam uma forma de BYOD
- ~36% das organizações têm os colaboradores acessíveis, mesmo não disponibilizando um meio de contacto
- ~67% dos colaboradores usam dispositivos próprios no emprego
- ~95% das organizações permite a utilização de dispositivos pessoais no local de trabalho

Via https://techjury.net/blog/byod-stats/

Como é que as organizações vêem o BYOD

- Os utilizadores são responsáveis
- Os utilizadores fazem uma gestão responsável dos seus dispositivos
- Os utilizadores estão conscientes dos riscos de segurança a que estão expostos e ajudam a proteger a organização

Como é que os utilizadores vêem o BYOD

- É o **meu** dispositivo
- Não é gerido centralmente pela entidade onde o vou utilizar. Sou **Eu** que faço a sua gestão.
- A entidade onde o vou utilizar tem pouco (ou nenhum) controlo sobre o que lá está instalado. **Eu** tenho o controlo.

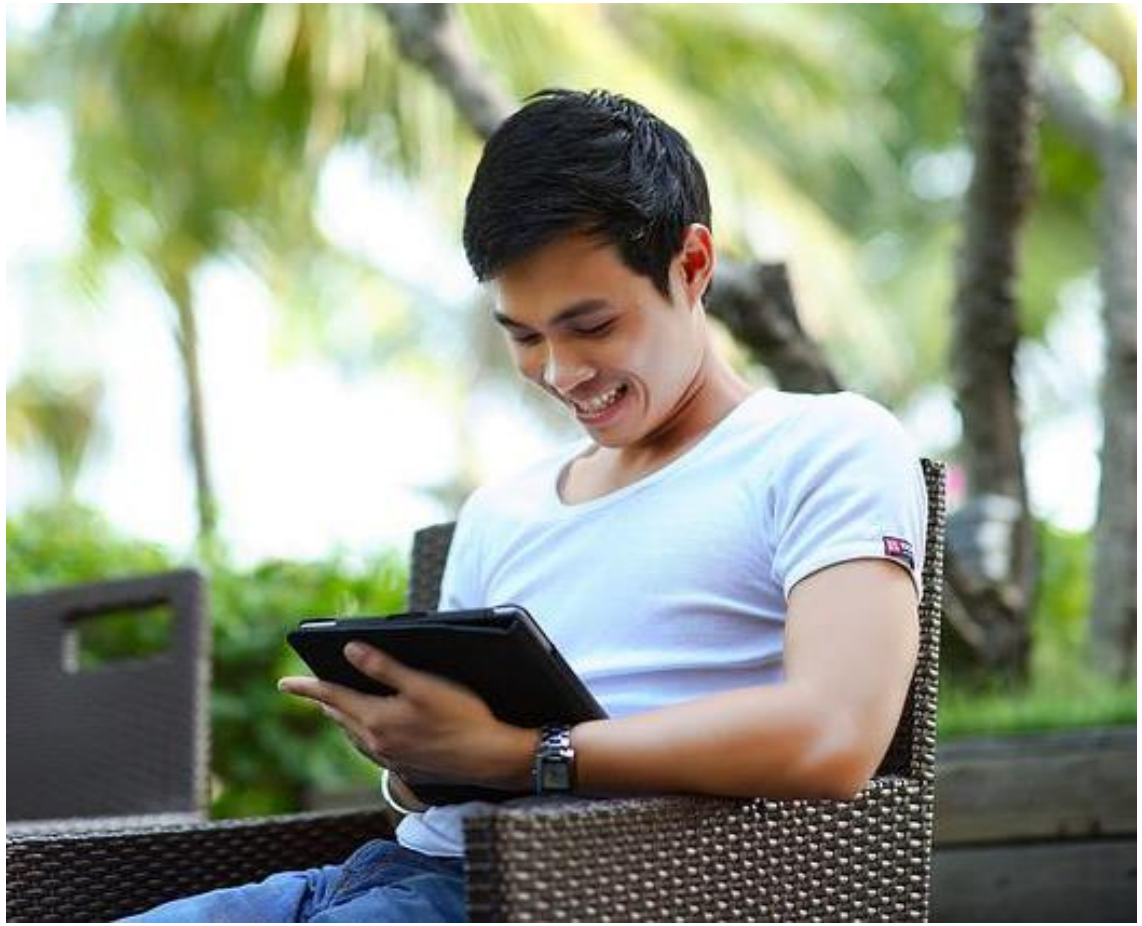

O LADO NEGRO DO BYOD

“O WiFi está lento. Não consigo trabalhar assim”

- O perímetro de segurança numa implementação de BYOD é muito maleável...
  - Os utilizadores trazem equipamentos não geridos, em alguns casos até routers WiFi
  - Abrem mais possibilidades para utilizadores maliciosos
  - Os recursos da organização podem ficar disponíveis a terceiros fora dela

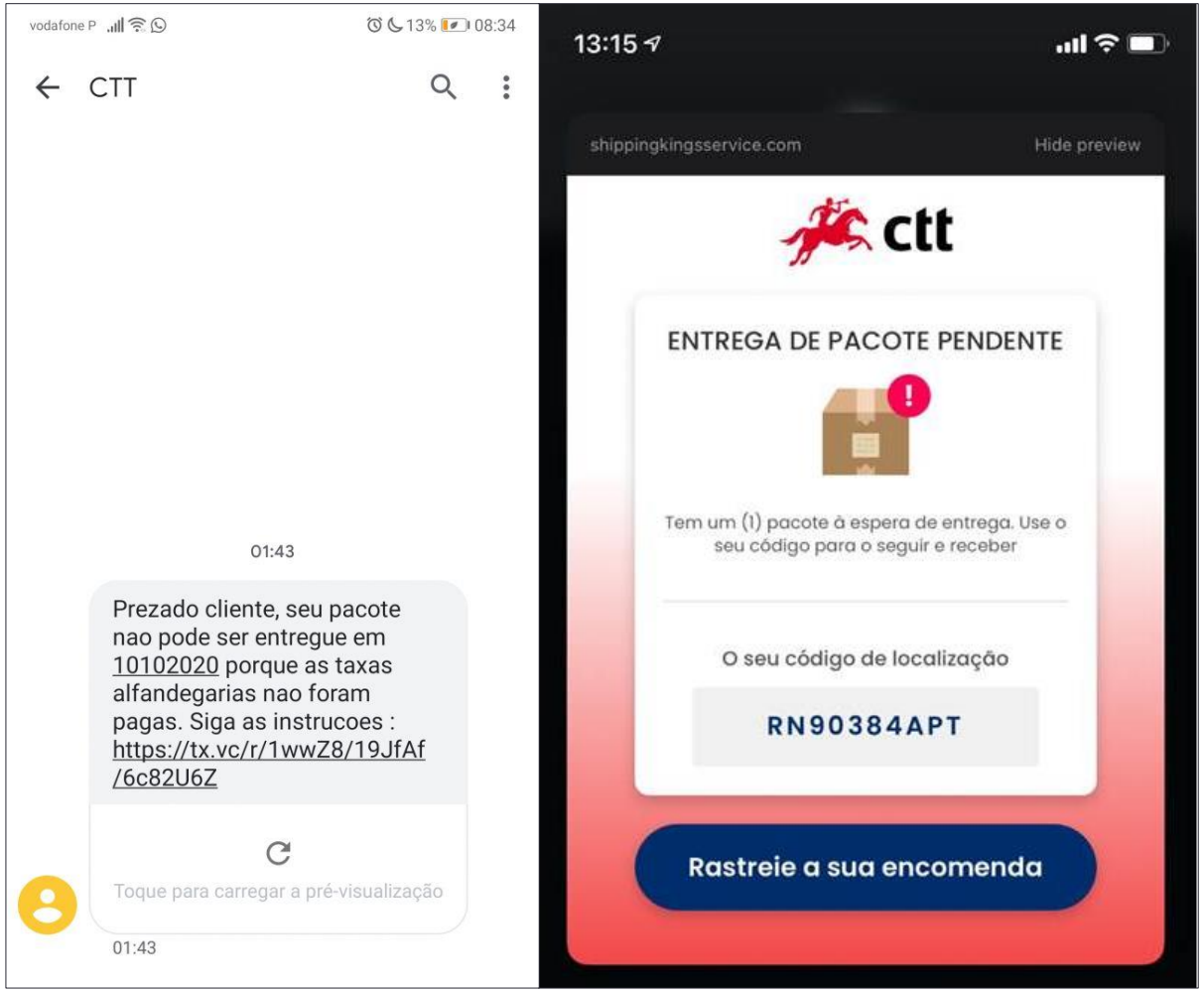
“Vou levar isto para trabalhar em casa”

- Quando os utilizadores querem ter acesso aos dados, onde quer que estejam...
  - Usam locais de armazenamento não autorizados pela organização (ex: Dropbox)
  - Enviam dados para as contas de correio electrónico pessoais
  - Descarregam os ficheiros para os seus dispositivos e não aplicam nenhuma proteção



“Não posso perder esta encomenda”

- É fundamental...
  - ...que os utilizadores saibam identificar ataques de SMShing e o Phishing para a segurança de uma prática de BYOD
  - ...que as organizações reconheçam a necessidade de consciencializar os seus utilizadores sobre o método correcto de actuação perante estas ameaças



“Vou só ali ao café”

- O roubo de equipamento é um dos principais problemas de segurança das organizações, com ou sem BYOD, mas...
  - Os utilizadores tendem a ter mais cuidado com os equipamento que não são deles
  - Os dispositivos dos utilizadores, tipicamente, não têm os mecanismos de proteção antiroubo aplicados nos dispositivos empresariais (p.ex.: cifra de disco)

“Não fui eu que trouxe isso”

- Com a maior proliferação do BYOD os atacantes também se adaptaram...
  - O *malware* pode ser preparado para atacar dispositivos diferentes daqueles em que é transportado
  - Os dispositivos tornam-se, efetivamente, cavalos-de-Tróia quando a segurança é descurada.


O CAMINHO EM FRENTE

Takeaway 1 – estamos nisto juntos

- A organização deve apoiar os utilizadores a tomarem decisões corretas, informando-os e educando-os de forma contínua
- Os utilizadores devem assegurar que os seus dispositivos estão devidamente geridos
- As regras e boas práticas devem ser conhecidas e acordadas entre ambas as partes

Takeaway 2 – eles andam aí

- Não é expectável que o crime no ciberespaço desapareça nos próximos tempos, antes pelo contrário

- Organizações e utilizadores devem estar conscientes dos métodos utilizados pelos criminosos e identificar proactivamente os riscos de segurança

Obrigado pelo vosso tempo

Q&A

Contactos


jorge.pinto@ap2si.org


linkedin.com/in/jorgepinto


twitter.com/infoseconlinept