



RNEP-GW

MÓDULO CIBERHIGIENE



CUIDADOS HABITUAIS, MENSAGENS

Proveniência de alguém conhecido ou desconhecido?

- Se desconhecido, existe um contexto plausível?

Olhar com atenção para o endereço de onde o e-mail foi enviado

A linguagem usada na mensagem é «normal»?

Só abrir o e-mail (e anexos) se esse contexto existir



CUIDADOS HABITUAIS, MENSAGENS

Se a mensagem parecer estranha, trocar impressões com outros colegas

- No sentido de averiguar se receberam uma similar



Caso se queira analisar de forma independente:

- Usar o www.virustotal.com
- Olhar para os cabeçalhos da mensagem



No caso de a dúvida persistir deve contactar a equipa de segurança da sua instituição

CUIDADOS HABITUAIS, MENSAGENS

EXAMPLE OF PHISHING EMAIL

Fri 12/11/2015 10:33 AM

Urgency

Critical System Maintenance Team '<noreply@csmt.com>

URGENT: Critical System Maintenance - Validate user account

To [redacted] → Not sent to you.

Follow up. Start by Friday, December 11, 2015. Due by Friday, December 11, 2015.
This message was sent with High importance.

Dear user, → Not addressed directly to you.

We are about to carry out maintenance on our user interface. Upon the receipt of this notice, you are required to validate users can access the interface.

Failure to validate account functions within this time duration, will inactive all user accounts. → Contains 'threat' if you don't act on email.

To validate the user interface, click on the web-link below or copy the link in your web-browser:

<http://reviewuserinterface.com/verify> → Attempts to direct you to a link

Yours in service,

Critical System Maintenance Team

CUIDADOS HABITUAIS, PASSWORDS

Não partilhar



Não escrever passwords em post-its

Não reutilizar



fnac

AT
autoridade
tributária e aduaneira



CUIDADOS HABITUAIS, PASSWORDS

Use segundo fator de autenticação (2FA) sempre que disponível

Utilização de software de gestão de passwords



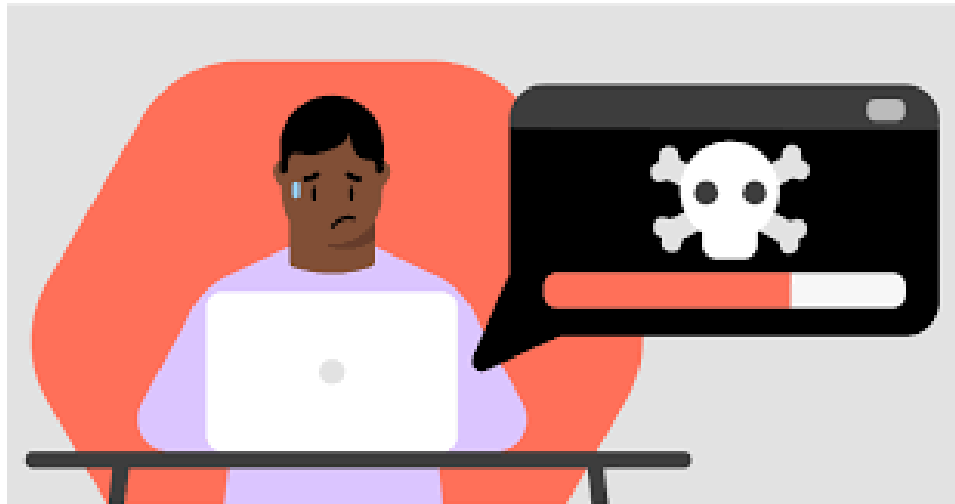
BACKUPS

Realize com frequência e mantenha os dispositivos offline depois de concluir o backup



NÃO INSTALAR SOFTWARE AD-HOC

Fazê-lo pode desencadear uma infecção de malware



ACTUALIZAÇÕES

São importantes para inibir vulnerabilidades



CARREGAMENTOS EM PÚBLICO

Podem potenciar infecções ou roubo de informação. Proteja-se.



CÓDIGOS QR

Códigos QR podem redirecionar para sites maliciosos ou instalar malware.



IDEIAS CHAVE



A proveniência de cada mensagem deve ser analisada com cuidado



As passwords são um vector importante, não se devem repetir em diferentes plataformas e sempre que possível usar 2FA



Fora do nosso ambiente é necessário algum cuidado, com portas USB para carregar dispositivos ou com códigos QR



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc