Para sua segurança, mude os seus comportamentos *online*

A sua saúde virtual depende de si.

Navegue em segurança!

Ocupar o tempo a transferir fundos de uma conta para a outra e receber uma comissão por isso não é um emprego. É crime!

Não sirva de *money mule*.

Dinheiro fácil é dinheiro perigoso!

Não seja cúmplice do crime organizado.
Desconfie de anúncios de emprego mal escritos, com erros gramaticais e ortográficos, que oferecem avultadas quantias de dinheiro e cuja interação e transação é exclusivamente *online*.
Verifique SEMPRE os dados das empresas que lhe fazem ofertas.

Tenha cuidado com os *negócios* e transações com recurso a dinheiro virtual.

Investir em bitcoins através da *internet* pode ser perigoso. Utilize-as apenas em sites credíveis e devidamente certificados para o efeito.

Nunca forneça os dados do seu cartão se não for para comprar algo.

E não grave os dados para pagamentos futuros.

Nunca adicione um número de telefone estranho à sua conta bancária.

O número de telefone dá acesso direto à movimentação da sua conta. Tenha MUITO cuidado.

Não forneça o código de ativação ou pin de acesso à aplicação MBWAY.

Não guarde no telefone informações sobre cartões de crédito ou multibanco.

Nunca clique num link de resposta de mensagens suspeitas.

Não faça download de softwares *estranhos*.

Não dê informações privadas mesmo que lhe digam que a entidade é fidedigna.

Suspeite sempre de chamadas não solicitadas.

Tenha cuidado com os perfis falsos nas redes sociais e com a simulação de relações amorosas.

Não envie dinheiro. Não forneça dados pessoais ou bancários.

Perfis com fotografias de pessoas atraentes funcionam como isco para conseguir a sua atenção.
Não se deixe enganar.
Acautele-se com e-mails desconhecidos pois são uma porta de entrada para o seu aparelho.
Não se deixe pescar!
Proteja-se do *phishing*, *smishing* e *vishing*.
Não revele a NINGUÉM os seus dados pessoais!
Não use o endereço de e-mail nem a mesma password nas redes sociais e na rede profissional.
Não misture a vida profissional com a vida pessoal!
Proteja-se do *hacking*.

Efetue cópias de segurança, mantendo os meios desligados após a realização da cópia.

O *ransomware* não acontece só nos filmes.

Não dê acesso remoto a desconhecidos.

Mantenha os seus dados em segurança. Inacessíveis.

Tenha cuidado com os e-mails de empresas fornecedoras ou altos responsáveis (CEO) a pedir para alterar dados bancários ou para fazer pagamentos para outra conta.

Suspeite.

Use meios alternativos para confirmar.

Denuncie.

Tenha cuidado quando acede a redes wi-fi públicas.

Procure não aceder a dados confidenciais.

Fotografar ou filmar outras pessoas sem consentimento é crime!

Não carregue nem descarregue fotos nas redes sociais.

Se não tem autorização para aceder, não aceda!

“Ter ficado ligado” não é desculpa.

Procure não expor os seus filhos nas redes sociais.

Lembre-se que não controla quem está do outro lado a ver.

Tenha atenção ao ciberbullying. Não deixe que aconteça aos seus filhos.

Não *deixe andar*.

Guarde endereços.

Capture écrans.

Não responda de volta.
Faça queixa na Polícia ou no M. P.

Usar ferramentas tecnológicas com o objetivo de perseguir ou assediar uma pessoa é crime.

Capture écrans.
Não responda de volta.
Denuncie.