ALERTA CIBERCRIME

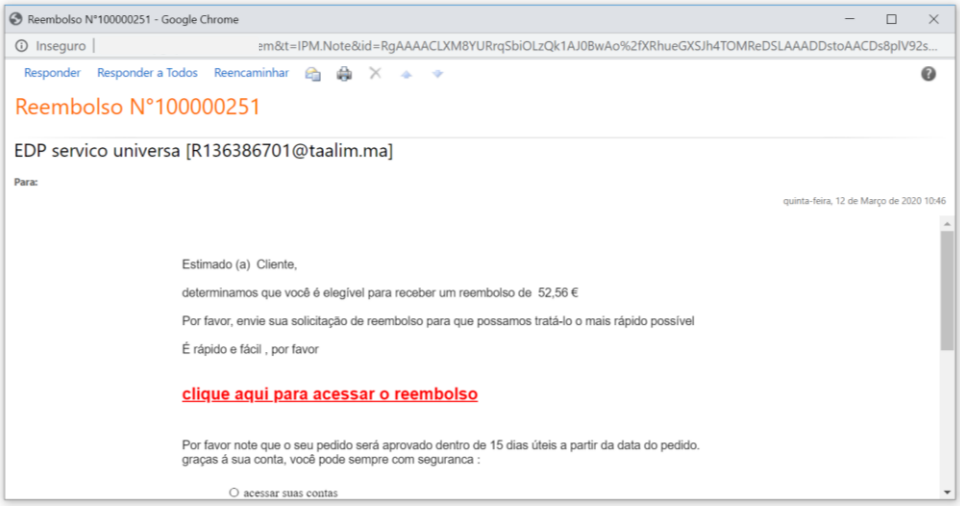
16 de março de 2020

'*Phishing*' dirigido a clientes da EDP e a titulares de cartões de crédito

1. Está em curso uma campanha de *phishing*, dirigida a vítimas que sejam simultaneamente clientes da *EDP* e titulares de cartões de crédito *Visa*, *Mastercard* ou *JCB*. Nesta campanha, os seus autores pretendem convencer as vítimas a facultar-lhes dados dos seus cartões de crédito, com o argumento de que pretendem reembolsar-lhes quantias.

2. Como habitual em casos de *phishing*, o processo começou com a expedição, para muitos destinatários, de mensagens fraudulentas de correio eletrónico. Foram registadas mensagens desta natureza desde o início do mês de março de 2020 e foi sinalizada pelo Gabinete Cibercrime uma concreta mensagem desta campanha expedida a 12 de março de 2020, pelas 10 horas e 46 minutos.

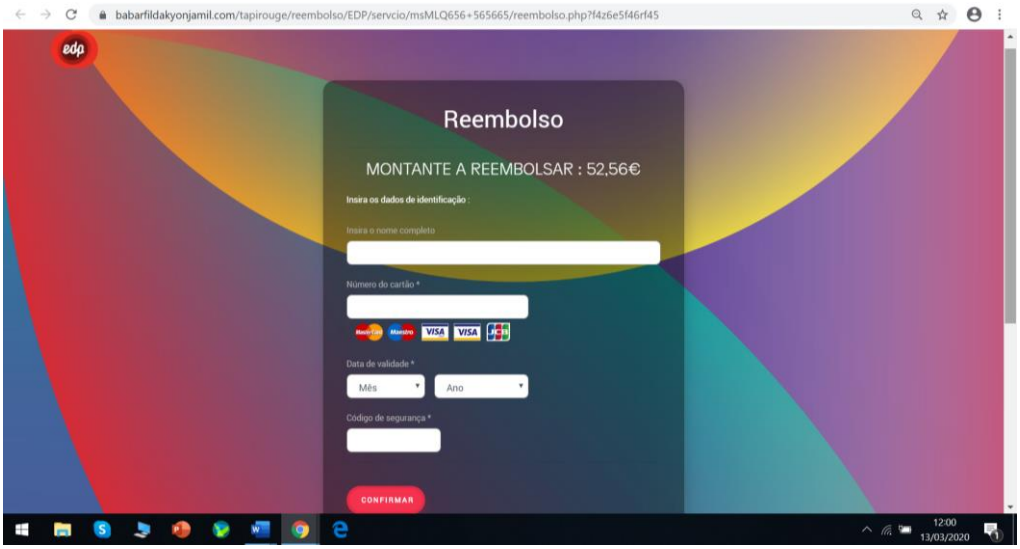
3. Nestas mensagens, com o título, no assunto "*Reembolso N°100000251*", anuncia-se que o destinatário, cliente da *EDP*, irá "*receber um reembolso de 52,56 €*". Para o efeito, indica-se de seguida um *link*, assinalado com a expressão "*clique aqui para acessar o reembolso*". As mensagens vêm assinadas com a expressão "*EDP serviço universal, Diretor de operações*".



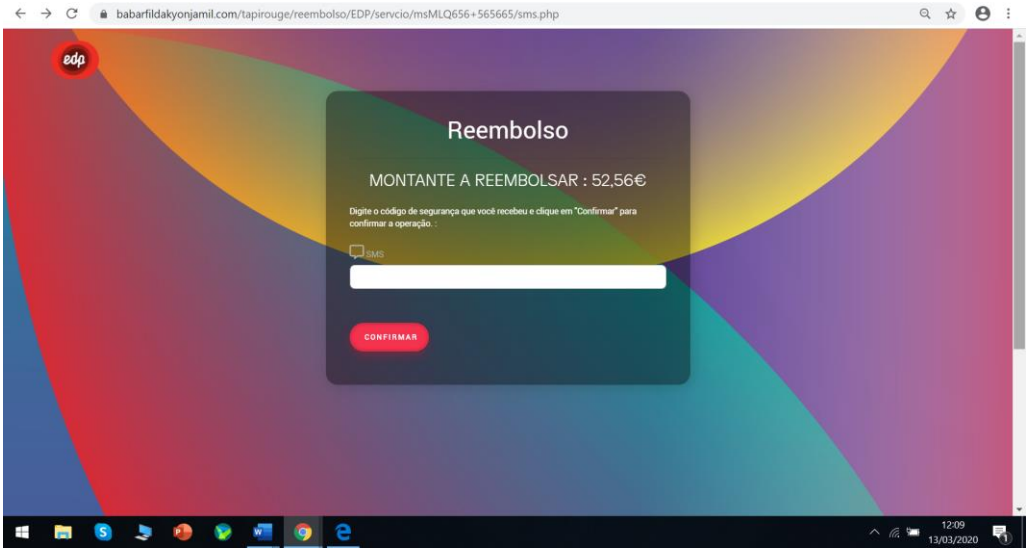
4. Trata-se, evidentemente, de mensagens fraudulentas, não provenientes da *EDP*. Não foram remetidas pela *EDP* nem a partir de sistemas informáticos pertencentes a esta companhia.
Aparentemente, tais mensagens foram remetidas da caixa de correio "*EDP servico universa*", mas na verdade provieram do endereço R136386701@taalim.ma. É um endereço de correio eletrónico de

uma plataforma pertencente ao Ministério da Educação Nacional de Marrocos, sendo a mensagem em causa efetivamente originária de um endereço de IP pertencente ao fornecedor *Aruba S.p.A. - Cloud Services* (https://www.arubacloud.com), companhia com sede em Itália, especializada em prestar serviços na *cloud* e *datacenters* em Itália, França, Espanha, Hungria, Polónia e México.

5. Por sua vez, o *link* que se referiu, contido nas mensagens fraudulentas, conduz a um s*ite* Internet que aparenta ser o da *EDP*, exibindo aparência gráfica e um logotipo normalmente utilizados por aquela companhia.
Além disso, inclui espaços em que se solicita a introdução de dados da vítima: o seu nome completo, o número do seu cartão de crédito, a respetiva data de validade e ainda o seu código de segurança.



Caso o utilizador introduza todos estes dados, abre-se uma nova página em que é solicitada a introdução do "*código de segurança que você recebeu*". Porém, a vítima não recebe qualquer código – nem o mesmo é enviado. Aliás, de seguida surge uma nova página com a mensagem "*o código digitado está incorreto ou expirou, um novo código foi enviado a você*."



6. Este *site* não é gerido pela *EDP* nem é por ela autorizado. Trata-se de uma página falsa, que pretende imitar a autêntica página da EDP. *Tem* como único propósito capturar os dados de cartão de crédito das vítimas.
Esta página fraudulenta está registada no fornecedor de serviços "*Tucows Domains Inc*." (http://tucowsdomains.com), com sede em Toronto, no Canadá, especializado no fornecimento de nomes de domínio e outros serviços de Internet.

7. Como se disse, esta página pretende imitar a aparência, aos olhos do utilizador comum, da autêntica página da *EDP*. Se a vítima aceder a ela e nela introduzir a informação que se lhe solicita, fornecerá aos autores destes factos todos os dados do seu cartão de crédito, permitindo assim àqueles que utilizem livremente este cartão, em compras ou pagamento de serviços.