Prevenção e combate às burlas são uma longa e importante tarefa, é necessária a participação de toda a população no combate às burlas

Nos últimos anos, as burlas através de telecomunicações e cibernéticas têm aumentado globalmente, o que prejudica gravemente a segurança dos bens e os legítimos direitos e interesses da população em todo o mundo, incluindo Macau.

Segundo os dados da Polícia Judiciária (PJ), nos primeiros oito meses deste ano, registaram-se 240 casos de burla telefónica, um aumento de 2,3 vezes em relação ao ano anterior, mais de 60% dos quais foram burlas de “falso funcionário de órgãos governamentais”. No mesmo período, registaram-se 488 casos de burla cibernética, o que representa um aumento de 23% face ao ano anterior, os quais foram principalmente burlas de investimento online “Sha zhu pan”, namoro online, compras online de produtos e de bilhetes de concertos e aumento do registo de encomendas, entre outros. As burlas informáticas de furto de dados de cartões de crédito para fazer compras online voltaram a aumentar, tendo-se registado 216 casos, o que representa uma subida de 1,4 vezes em comparação com o ano anterior, e em muitos desses casos os dados dos cartões de crédito das vítimas foram furtados através de websites falsos. Quanto à extorsão de “nude chat”, registaram-se 68 casos, um aumento de 51% em relação ao ano anterior. Estes casos causaram, no total, um prejuízo de mais de 160 milhões de patacas, quase o dobro do ano anterior.

Fundamentalmente, a principal razão da alta ocorrência de burlas é a escassa sensibilidade de uma parte da população na prevenção de

burlas. Embora a polícia, os serviços e as entidades governamentais competentes e as associações particulares divulguem alertas e efectuem acções de sensibilização, de forma plena e ininterrupta, uma parte da população ainda não está atenta, caindo em armadilhas de burla extremamente comuns, e algumas pessoas até são convencidas a participar no crime sem saberem que estão a ser burladas.

Por outro lado, a maioria das actividades sociais, de comunicações e de compras do público em geral são feitas via internet, o que tem criado oportunidades para que sejam praticados crimes com recurso às telecomunicações e ao espaço cibernético. Ao mesmo tempo, os criminosos usam meios mais enganadores e específicos para praticar os crimes, o que dificulta a prevenção. Assim, é necessário melhorar a consciencialização de toda a sociedade neste âmbito e, em especial, melhorar o conhecimento sobre os novos modi operandi, para que seja possível identificar de imediato uma burla.

Neste artigo resumimos dois tipos de burlas através de telecomunicações e cibernéticas que têm surgido frequentemente nos últimos meses, que são altamente enganosas e com modus operandi complexo e mutável, de modo a alertar a população para estar mais atenta a estes crimes e assim assumir melhor a responsabilidade de proteger a segurança dos próprios bens.

I. Cuidado com os novos esquemas da burla de investimento online, conhecida por "Sha zhu pan"

O novo modus operandi da burla de investimento online "Sha zhu pan" consiste num esquema em que os burlões procuram alvos nas

plataformas sociais, websites de relacionamento, entre outros, para ganhar a confiança das vítimas. Depois, a pretexto da oferta de "dicas" para investimento em acções, planos de investimento com alto rendimento e informações sobre as vulnerabilidades de segurança dos websites do jogo online, aliciam as vítimas para as fazer cair em armadilhas de falsos investimentos ou de falsas apostas. No início as vítimas fazem pequenas apostas e conseguem ganhar, mas, assim que aumentam o valor das apostas, os burlões entram em acção, conhecida vulgarmente como "colheita" ou "abate", conseguindo assim burlar as vítimas em grandes quantias.

Recentemente, uma grande variedade de novos esquemas da burla de investimento online “Sha zhu pan” tem aparecido em Macau, nomeadamente:

1. **Partilha da experiência de investimento de “celebridades”:** os burlões fazem numerosas acções de publicidade nas principais plataformas sociais, fazendo-se passar por personalidades ou especialistas na área financeira que ensinam estratégias de investimento e que partilham experiências, a fim de atrair os internautas para se juntarem aos grupos de comunicação, após o que divulgam de forma contínua notícias sobre lucros para induzir a participação dos membros em falsos investimentos e assim concretizar a burla.

2. **Mensagens de amigos fictícios:** os burlões enviam mensagens, de forma aleatória, aos utilizadores de telemóvel. Os burlões, para começar a conversa, nessas mensagens mandam cumprimentos em nome de um amigo, ou a pretexto de fazerem amigos ou de

prestarem serviços de consultadoria. Se a vítima responder, o burlão procura, de forma constante, assuntos para continuar a conversa e ganhar a confiança da vítima. A seguir, o burlão induz a vítima a fazer um investimento falso.

3. **Mensagens de falsos investimentos:** os burlões enviam mensagens, de forma aleatória, aos utilizadores de telemóvel, passando-se por técnicos analistas de uma empresa de investimentos ou de um banco, dizendo que têm um projecto de investimento onde se pode ganhar muito dinheiro, induzindo a vítima a clicar num link indicado na mensagem para ter um contacto, a fim de praticar a burla.

O novo tipo de burla de investimento online “Sha zhu pan” assenta em saber aproveitar a confiança do público nas celebridades, a curiosidade de fazer amigos e a necessidade de ter amigos pela internet, assim como no desejo do investimento de alto rendimento. Antes da “colheita”, ou seja, antes de obterem ilicitamente o dinheiro através da burla praticada, os burlões são bastante pacientes e trabalham para ganhar a confiança das vítimas, o que acaba por ser um aspecto muito tentador. Assim, para prevenir este novo tipo de burla de investimento online “Sha zhu pan”, a população deve ter em mente o seguinte:

1) Não confiar em qualquer identidade alegada por estranhos; não responder a mensagens de amigos fictícios ou relativas a investimentos de origem desconhecida e bloquear o autor dessas mensagens;

2) Não participar em actividades de investimento em acções ou em criptomoeda de origem desconhecida, nem acreditar cegamente em

anúncios ou projectos na rede sobre investimentos com lucro elevado, uma vez que estes investimentos, que alegadamente irão gerar ganhos avultados com pouco dinheiro ou que irão ser lucrativos e sem perda de dinheiro, o que serve para atrair as pessoas, são frequentemente burlas;

3) Não clicar em links anexados a mensagens ou posts de origem desconhecida nas redes sociais e, se forem convidados para um grupo de comunicação sobre investimentos, não aceitar e bloqueá-lo o mais rapidamente possível.

II. Cuidado com websites falsos e quaisquer mensagens com links que direccionem para outro website

Nos últimos anos, continua a ser grande a incidência dos casos de uso ilícito de cartões de crédito, e a criação de websites de phishing é o principal meio usado pelos criminosos para subtrair os dados dos cartões de crédito, seja através das particularidades dos websites, sejam os meios utilizados para aliciar as pessoas a clicar, sejam os métodos de propagação, todos são altamente tentadores. Ultimamente verificam-se também falsos programas de instituições financeiras para telemóveis. Assim, para evitar o furto de dados pessoais, de dados das contas online ou de cartões de crédito, todos devem ser mais cautelosos.

1. As referências (fictícias) usadas nos websites de phishing estão, muitas vezes, intimamente ligadas à vida quotidiana da população, como exemplo, páginas de softwares de comunicação dominantes, equipamentos informáticos de renome, empresas de serviços cibernéticos, serviços públicos, instituições financeiras, companhias de correio rápido e de transporte logístico,

estabelecimentos de venda a retalho dos supermercados, entre outros, e tanto as páginas iniciais como os endereços dos websites falsos são muito parecidos com os dos websites verdadeiros.

2. Os criminosos usam diferentes pretextos para aliciarem as vítimas a clicar em websites falsos e a introduzir dados, designadamente com a ameaça de suspensão ou proibição do uso das contas, a falha no envio de encomendas que implica o pagamento de taxas postais, incitamento a fazer o login em contas para participar em sorteios, entre outras formas de ameaças e aliciamentos.

3. Os criminosos compram anúncios publicitários para que os websites falsos possam ser colocados no topo dos resultados de pesquisa nos motores de busca mais usados, ou criam nas plataformas sociais muitas páginas electrónicas falsas ou contas, extremamente parecidas às verdadeiras, ou enviam aleatoriamente mensagens ou emails com links de falsos websites, com vista a aliciar a população a aceder aos websites de phishing e furtar os dados.

Para evitar os prejuízos provocados por furto de dados, a população deve estar atenta ao seguinte:

1. Embora o fornecimento online de dados seja comum, é necessário estar atento à protecção dos próprios dados pessoais, e sempre que seja solicitada a introdução de dados pessoais, de conta online, financeiros ou de cartões de crédito, a população deve estar especialmente alerta e verificar com cautela a veracidade do website, e se considerar necessário pode solicitar uma confirmação oficial.

2. Reforçar ainda mais as medidas de prevenção, como usar o código de verificação de utilização única em pagamentos com cartão de crédito, utilizar a autenticação de dois factores nas contas online. Se, por inadvertência, forem fornecidos dados num website de phishing, deve ser suspenso de imediato o uso do cartão de crédito e aceder-se à conta online para alterar a senha, com vista a efectuar a sua recuperação.

3. Nunca e em momento algum se deve clicar num link de websites não identificados ou fazer, irreflectidamente, a leitura de um código QR.

Para além dos dois novos tipos de burla que ultimamente têm ocorrido com frequência, outras burlas online, tais como burlas telefónicas em que alguém se faz passar por funcionário de órgãos de segurança pública, burlas de namoro online, de “aumentar o registo das encomendas”, de compras online, bem como a extorsão de “nude chat”, entre outros, que causam uma ameaça enorme não só para a segurança dos bens como também para os legítimos direitos e interesses da população, que deve continuar a manter-se alerta, sem baixar a guarda. A população deve trocar sempre informações sobre prevenção da burla com a família e com os amigos, de modo a alertarem-se uns aos outros. **Para consultas ou apoio, o público pode telefonar para o nº 8800 7777, linha aberta para a prevenção de burlas da PJ. Quando, lamentavelmente algum membro do público perceber que foi ele próprio burlado, ou um amigo seu, deve fazer, de imediato, a denúncia, para que a PJ possa proporcionar o apoio adequado e iniciar o eventual processo de recuperação do dinheiro furtado.**