Tendências da criminalidade cibernética durante a pandemia e estratégias para a sua prevenção

A situação da epidemia de Covid-19 teve um impacto grave sobre o modelo original de actividades económicas e de vida da população em toda a parte, e também mudaram quer o modo de vida e os hábitos das pessoas, quer as suas actividades sociais diárias, de aprendizagem, de trabalho e de entretenimento, que migraram rapidamente para a internet. Entre estas actividades, as compras online têm-se desenvolvido a um ritmo ainda mais rápido, devido às vantagens de conveniência, diversidade, transregionalidade e ausência de contacto pessoal. Mais, com a crescente popularização do pagamento online e do pagamento móvel, as compras na rede tornaram-se, desde o início da pandemia, uma realidade indispensável da vida quotidiana das pessoas. No entanto, a rápida popularização das compras online não só cria facilidades para o público, como também cria oportunidades para os criminosos praticarem burlas online e furtarem dados cibernéticos pessoais, o que constitui uma séria ameaça para a privacidade e para os interesses patrimoniais das pessoas.

Principais tipos de crimes relacionados com as compras online e as suas características durante a pandemia

Desde o início da pandemia que se verificou em Macau um aumento exponencial do número de crimes relacionado com as compras online, número esse que pode ser dividido em dois grandes grupos, conforme o modus operandi e os crimes. Um deles é a burla informática (artigo 11.º da Lei de combate à criminalidade informática), praticada através do furto dos dados constantes dos cartões de crédito, com o objectivo de

serem feitas compras online, o outro é a burla (artigo 211.º do Código Penal), praticada a pretexto de compras feitas na rede.

No primeiro tipo de casos, os criminosos começam por usar meios como os phishingsites, propagação de programas Trojan e falsos serviços de pós-venda para burlar ou para furtar os dados dos cartões de crédito das vítimas durante as compras online, e posteriormente utilizam esses dados dos cartões de crédito para fazer compras online ou para jogar online e assim obter benefícios. Além disso, nos últimos anos, têm-se registado, ocasionalmente, casos de vazamento de dados em sites de compras online e plataformas de redes sociais de grande envergadura, o que teve como consequência a transferência de uma grande quantidade de dados de cartões de crédito para a “dark web”, onde foram postos à venda. Em anos anteriores este tipo de casos não era muito frequente, contudo, subiu significativamente devido ao aumento, após o início da pandemia, do número de consumidores online. Em 2020 e 2021, foram registados 411 e 663 casos, respectivamente, o que representa um aumento notável em comparação com os 117 casos de 2019, antes da pandemia. Os processos denunciados em 2021 causaram perdas superiores a 7,42 milhões de patacas, o que reflecte os perigos ocultos e os riscos decorrentes do aumento das actividades de compras online durante a pandemia.

O segundo tipo de casos é mais semelhante ao crime de burla tradicional, e os criminosos visam, directamente, o dinheiro ou as mercadorias das vítimas, sendo as compras online apenas um método ou meio que utilizam para se aproximarem e ganhar a confiança das

vítimas. Nos casos em que os burlões se fazem passar por vendedores, costumam publicitar,em grupos ou em páginas das redes sociais e em fóruns online, a venda de produtos promocionais ou de edição limitada, burlando as vítimas através do método “pagamento antes da entrega de mercadorias”. Com o surto do Covid-19, este tipo de burla aumentou de forma exponencial, tendo-se registado, no início da pandemia, vários casos de burla ligados à venda de máscaras e de material médico. Em 2020, foram instaurados na PJ 114 processos de burla de compras online, que incluíam também compras de máscaras online, quase o dobro do número de 2019. Em 2021, registaram-se 95 casos deste tipo, e apesar de o número ter diminuído em comparação com o período homólogo do ano anterior, continua a ser superior ao número de processos anterior à pandemia. Entre as denúncias, para além das burlas ligadas a material médico, verificaram-se ainda vendas falsas de produtos de moda, acessórios de luxo, produtos electrónicos, alojamento em hotéis, cupões para restaurantes, bilhetes de concertos, entre outros. Em relação aos burlões que se fazem passar por compradores, são geralmente casos com origem nas regiões vizinhas. Os malfeitores começam por procurar vendedores através de plataformas ou grupos nas redes sociais, alegando que desejam comprar os produtos, após o que recorrem a transferências falsas, cheques revogáveis ou registos de transferências que simulam o pagamento e, muitas vezes, os vendedores só descobrem que o pagamento não chegou a ser efectuado depois do envio dos produtos. Dada a variedade de modus operandi deste tipo de burlas, o público deve avaliar com prudência os riscos e ter a maior atenção ao efectuar compras ou vendas online.

Estratégias de resposta aos crimes relacionados com as compras onlinedurante a pandemia

Perante a situação do aumento acentuado, nos últimos anos, dos crimes associados às compras online, nomeadamente, os casos de burla ligada a cartões de crédito, que num curto período de tempo são numerosos, têm um impacto amplo e envolvem muitas vítimas, com vista a controlar de forma abrangente este tipo de crimea Polícia tem ajustado as acções e concretizado estratégias de resposta dinâmica, que dão tanto relevo ao combate como à prevenção.

Quanto ao combate às burlas com recurso a cartões de crédito, a Polícia melhora constantemente a capacidade de investigação e de associação de diferentes casos em função das semelhanças verificadas entre eles, intensificando, também, a troca de informações com as polícias de outras jurisdições, assim comotem mantido uma cooperação próxima com o sector bancário no que diz respeito às burlas, e todas estas acções têm produzido efeitos na identificação da origem da fuga de dados dos cartões e das plataformas online onde se efectuam transacções com os dados furtados, bem como na identificação de grupos criminosos, do seu modus operandi e das pessoas envolvidas, com vista a efectuar um combate específico a este tipo de criminalidade. A título de exemplo, na sequência dos casos ocorridos no segundo semestre de 2018, a PJ desenvolveu uma investigação profunda e realizou uma operação, em Janeiro de 2019, que culminou com a detenção de sete elementos de uma rede criminosa. A par disso, a partir de 2020, a PJ participou, em colaboração com a Polícia de Hong Kong, em três acções da “Operations Soaring Star”, que desmantelaram vários

grupos que se dedicavam à prática de crimes cibernéticos transfronteiriços e que funcionavam em HK e em Macau. Ao mesmo tempo, a Polícia também se dedica a acções de sensibilização referentes à prevenção criminal. Neste âmbito foram realizadas, num total de 176 sessões, palestras relativas à prevenção da criminalidade informática e cibernética, onde foi explicado, junto de cerca de 24000 participantes, o modus operandi mais recente e foram transmitidos conhecimentos sobre prevenção. Por outro lado, continuam a ser divulgadas, online e offline, informações anticrime, para melhorar consideravelmente a sensibilidade e a capacidade de prevenção do público. Face à diminuição do número de casos, conclui-se que as medidas de combate e prevenção utilizadas têm vindo a produzir efeitos pois originaram uma clara descida deste tipo de crimes a partir do terceiro trimestre do ano passado.

Embora a situação geral do crime informático tenha melhorado claramente no primeiro semestre do corrente ano e em comparação com o ano anterior tenham diminuído os referidos dois tipos de crime relacionados com compras online, a actual conjuntura da segurança do espaço cibernético continua a ser complexa e preocupante. Existem armadilhas virtuais por todo o lado e surgem frequentemente vulnerabilidades de segurança de sites e de software, os meios usados na prática do crime cibernético mudam constantemente e, em contrapartida, o crescente grau de dependência que as pessoas têm deste meio de compras, para a maioria dos utilizadores da rede, não é acompanhado do aumento do sentido de protecção e da melhoria de técnicas para fazer frente ao crime cibernético. Esses factores de risco estão interligados, e não podemos subestimar a ameaça concreta que o

crime cibernético causa aos interesses do público. Face à situação actual, a Polícia vai continuar a melhorar a gestão da segurança do espaço cibernético e a reforçar a garantia de segurança das actividades públicas online. Em paralelo, os utilizadores da rede devem igualmente assumir as suas responsabilidades próprias e melhorar a sua capacidade de identificar diferentes armadilhas cibernéticas e de prevenir eventuais perigos online, especialmente deve continuar a aprofundar o seu conhecimento sobre a segurança cibernética e dos equipamentos informáticos, ter cuidado ao participar em actividades em redes sociais ou de consumo online, ter um melhor sentido de protecção dos seus dados pessoais e do seu património, resistir a actos ilegais praticados online, e trabalhar conjuntamente para a promoção do desenvolvimento saudável das diferentes actividades online a que se dedicam.