BAB V

PENUTUP

A. Kesimpulan

Berdasarkan hasil analisis dan pembahasan terkait praktik *quishing* dan *phising* dalam transaksis digital, dapat ditarik kesimpulan seperti berikut:

1. *Quishing* menggunakan *malware* dengan memanfaatkan kode QR untuk mengelabui korban dimulai dari pembuatan kode QR berbahaya yang ketika dipindai, akan mengarahkan korban ke situs *web* berbahaya atau memulai pengunduhan *malware*. Setelah *malware* terinstal, ia dapat mencuri data penting. Sementara *phishing* berbasis teks yang bermula dari pengiriman *email* palsu dari organisasi yang dikenal, meminta korban untuk memperbarui informasi mereka melalui tautan yang disediakan. Ketika korban meng-klik tautan, mereka diarahkan ke situs *web* palsu dan diminta memasukkan informasi pribadi untuk dikirim ke *phisher*. Kedua cara tersebut kemudian memungkinkan pelaku melakukan transaksi digital atas nama korban, menguras rekening bank mereka, dan menggunakan identitas mereka untuk aktivitas seperti pinjaman *online.*
2. *Moral hazard* berkaitan dengan perilaku, sifat dan karakter manusia yang dapat meningkatkan risiko kerugian. Hal ini sesuai dengan perilaku pelaku *quishing* dan *phishing* dalam transaksi digital yang sering kali didorong oleh sifat rakus dan tamak, sehingga menyebabkan kerugian pada korban. Mereka mencuri informasi pribadi atau keuangan dengan keyakinan akan terhindar dari tanggung jawab hukum, sehingga menciptakan risiko dan kerugian bagi korban. Perilaku *quishing* dan *phishing* termasuk dalam

kategori *moral hazard*, karena pelaku menghasilkan risiko atau kerugian bagi orang lain tanpa merasa bertanggung jawab atas konsekuensinya. *Moral hazard* mengandung 9 aspek antara lain asimetri informasi, insentif dan kontrak, pengawasan dan regulasi, kebijakan publik, pasar dan transparansi, manajemen resiko, budaya organisasi, konflik kepentingan, pencegahan dan mitigasi

3. Ditinjau dari Kaidah *ḍarar, quishing* dan *phishing* termasuk salah satu bentuk kemudharatan karena dampaknya sangat merugikan, baik secara finansial maupun dalam hal kehilangan privasi dan keamanan data. *Quishing* dan *phishing* menyebabkan bocornya data penting serta kerugian finansial yang signifikan bagi korban. Berdasarkan analisis ini, *quishing* dan *phishing* adalah bentuk perbuatan yang mengandung *darar* dan harus dihilangkan sesuai dengan kaidah fikih bahwa "*kemudharatan itu harus dihilangkan*."

   Ditinjau dari teori *ghish*, penulis menyimpulkan bahwa *quishing* dan *phishing* termasuk *ghish* (penipuan) untuk melakukan pencurian melalui teks dan gambar yang dapat menyebabkan pencurian identitas, di mana informasi pribadi korban digunakan untuk penipuan finansial, membuka akun baru, atau melakukan transaksi tanpa izin, serta mengakibatkan kerugian finansial bagi korban..

B. Saran

Dari kesimpulan uraian di atas, peneliti memberikan beberapa saran dan rekomendasi seperti berikut:

1. Bagi Pemerintah

   pemerintah perlu mengambil langkah-langkah proaktif yang meliputi:

   a. peningkatan kesadaran masyarakat tentang ancaman *cybercrime*, Peningkatan pendidikan dan pelatihan tentang keamanan *cyber* bagi masyarakat, terutama pengguna internet dan pelaku bisnis, akan membantu meningkatkan kewaspadaan mereka terhadap taktik penipuan quishing dan phishing.
   b. peningkatan pengawasan dan penegakan hukum yang tegas terhadap pelaku kejahatan *cyber* untuk mencegah serangan lebih lanjut dan memberikan efek jera bagi para pelaku
   c. peningkatan kerjasama antara pemerintah, sektor swasta, dan lembaga internasional dalam memerangi serangan *cyber* juga penting untuk mengembangkan solusi bersama dan pertukaran informasi tentang ancaman *cyber*crime yang sedang berkembang.

2. Bagi masyarakat

   Masyarakat diharuskan waspada serta penting untuk selalu memeriksa keaslian sumber atau pengirim pesan atau QR *code* sebelum melakukan interaksi atau mengklik tautan. Masyarakat juga harus lebih hati-hati dalam memberikan informasi pribadi atau keuangan melalui *email*, pesan teks, atau situs *web* yang mencurigakan.