Keamanan Transaksi Kartu Kredit di Internet

Penggunaan kartu kredit di Indonesia terus mengalami peningkatan setiap tahun. Terbukti, di dalam statistik Bank Indonesia terlihat adanya penambahan sekitar 1 juta kartu kredit dalam setiap tahunnya. Sampai pertengahan 2014, tercatat 15 juta kartu kredit telah digunakan oleh masyarakat Indonesia.

Dalam setiap peningkatan jumlah, terdapat pengguna-pengguna baru yang kali pertama mempunyai kartu kredit. Selain kegunaan yang umum sebagai alat pembayaran dalam pembelian di toko, pemesanan kamar hotel, cicilan produk, dan sejenisnya, terdapat aktivitas transaksi pembayaran melalui internet.

Namun banyak pengguna yang merasa khawatir perihal keamanan ketika melakukan transaksi di internet dengan kartu kredit.

Selain karena tidak ada edukasi dari bank penyelenggara kartu kredit bagi para pengguna pemula, juga banyak informasi negatif di masyarakat mengenai penyalahgunaan kartu kredit di internet.

Tidak heran, banyak masyarakat yang sampai saat ini memilih tidak menggunakan kartu kreditnya untuk bertransaksi di internet. Bahkan ketika terpaksa menggunakannya, pengguna kerap dihantui kekhawatiran akan risiko yang banyak diberitakan oleh media massa dan media sosial di internet.

Jika pihak bank penyelenggara kartu kredit bisa memberikan informasi yang jelas mengenai keamanan transaksi dengan kartu kredit, masyarakat pengguna tentu dapat lebih tenang dalam melakukan transaksi di internet. Dengan informasi yang benar, pengguna juga bisa menghindari kemungkinan negatif saat akan melakukan transaksi.

Komputer Pribadi

Ketika hendak melakukan pembayaran dengan menggunakan kartu kredit di internet, pertama-tama kita perlu memastikan bahwa komputer yang digunakan untuk melakukan transaksi pembayaran di internet adalah milik sendiri atau kita telah mengenalnya dengan baik.

Hindari melakukan pembayaran *online* menggunakan komputer publik, komputer sewa seperti warnet, atau meminjam komputer orang lain. Sebaiknya transaksi dilakukan melalui komputer pribadi untuk menghindari adanya program-program jahat yang menyimpan setiap tombol *keyboard* yang ditekan pada saat pembayaran.

Program yang dikenal sebagai *keylogger* ini bekerja menangkap segala ketikan yang terjadi di dalam *keyboard*. Jika semua data kartu kredit disimpan oleh program ini, maka pemilik program dapat dengan mudah menggunakan data tersebut untuk kepentingan transaksi di internet.

Program ini cukup banyak ditemukan di internet dan dapat digunakan secara bebas dan gratis. Sehingga kemungkinan *software* ini telah terpasang di komputer publik sangat besar. Sehingga pengguna disarankan untuk hanya menggunakan komputer pribadi dalam bertransaksi.

Kedua, kita perlu memastikan terlebih dahulu bahwa alamat *website* di dalam kotak alamat diawali dengan https dengan disertai gambar gembok yang terkunci. Jika tidak ada, sebaiknya tidak melakukan pembayaran di *website* tersebut.

Apabila keduanya telah muncul di dalam kotak alamat, maka *website* penyelenggara transaksi dapat dinilai telah menyediakan infrastruktur dengan baik. Keberadaaan https atau http secure adalah untuk mengamankan dari penyadapan data pada saat pengguna melakukan pembayaran.

Informasi yang disadap akan menjadi tidak berguna karena melalui protokol keamanan ini telah diacak atau disandikan sehingga tidak bisa dibaca secara langsung. Dengan demikian, Anda tidak perlu khawatir identitas kartu kredit dicuri oleh orang lain.

Ketiga, kita juga perlu memastikan nomor telepon dan alamat e-mail yang tercatat oleh bank penyelenggara kartu kredit merupakan data terbaru yang digunakan saat ini. Memperbarui data setiap kali terjadi perubahan akan menyelamatkan kita ketika terjadi transaksi palsu.

Dengan usaha tersebut, umumnya kita akan menerima pesan setiap kali terjadi transaksi menggunakan kartu kredit. Apabila transaksi yang diinformasikan tidak pernah dilakukan, maka dapat dengan cepat diantisipasi.

Keamanan 3D

Selain itu, ada manfaat yang lebih besar ketika melakukan transaksi pada *merchant* atau pengusaha *online* yang telah menerapkan 3D Secure dalam pembayaran kartu kreditnya.

Kode keamanan yang harus dimasukkan sebagai validasi pembayaran akan dikirimkan melalui pesan singkat ke telepon seluler pengguna kartu kredit.

Apabila kode keamanan tersebut tidak dimasukkan, maka proses pembayaran akan dibatalkan. Keterlibatan telepon selular yang ada di tangan pemilik akan semakin mempersulit penyalahgunaan kartu kredit.

Protokol keamanan yang awalnya dikembangkan oleh Visa dan telah diadopsi oleh MasterCard, JCB International, serta American Express ini telah banyak digunakan oleh berbagai situs belanja di internet.

Berbeda dari tiga digit kode keamanan yang melekat di belakang kartu kredit, kode keamanan dari 3D Secure selalu berganti-ganti sesuai dengan teks yang dikirimkan ke pemilik kartu kredit melalui telepon seluler.

Meskipun identitas kartu kredit berhasil dicuri, data-data tersebut tidak akan cukup berguna untuk melakukan transaksi tanpa disertai persetujuan pemilik melalui kode keamanan yang dikirim melalui telepon selulernya.

Perbaikan dan peningkatan keamanan dalam pembayaran *online* menggunakan kartu kredit akan membuat semakin mudah dan nyaman para penggunanya. Dengan demikian, kekhawatiran akan penyalahgunaan kartu kredit di internet dapat semakin diminimalkan. (38)

Ridwan Sanjaya,
dosen Sistem Informasi Unika Soegijapranata