E-Gold sebagai Alternatif Alat Pembayaran pada E-Commerce

P.A. Christianto
Fakultas Ilmu Komputer, Universitas AKI Semarang
p_a_chr@yahoo.com

Abstrak : Transaksi lewat internet bukanlah suatu hal yang asing lagi untuk saat ini, dimana e-Commerce sudah berkembang begitu pesat sehingga hampir setiap pengguna jasa transaksi online, menggunakan program bantu untuk memudahkan melakukan transaksi yang dinamakan "payment processor". Namun disisi lain, masih banyak yang beranggapan bahwa melakukan transaksi lewat internet tidaklah aman, di karenakan banyaknya kasus-kasus penipuan yang terjadi.
Sehubungan dengan hal tersebut, maka di perlukan pengetahuan tentang cara melakukan pembayaran lewat internet dengan menggunakan e-Gold, yang merupakan salah satu cara pembayaran lewat internet. Dalam pembayaran menggunakan e-Gold, pengguna dapat mengirim sejumlah uang kepada pengguna eGold yang lainnya tanpa perlu mengetahui nomor rekening atau nomor kartu kredit yang dituju.

Kata Kunci : E-Commerce, E-Gold

PENDAHULUAN

Istilah e-business berkaitan erat dengan e-commerce. Bagi sebagian kalangan, istilah e-commerce diartikan secara sempit sebagai transaksi jual beli produk, jasa dan informasi antar mitra bisnis lewat jaringan komputer, termasuk internet. Sedangkan e-business mengacu pada lingkup yang lebih luas dan mencakup pula layanan pelanggan, kolaborasi dengan mitra bisnis, dan transaksi elektronik internal dalam sebuah organisasi.

Meskipun demikian, istilah e-commerce sebenarnya dapat di definisikan berdasar 5 perspektif (Phan, 1998): (1) on-line purchasing perspective: Sistem yang memungkinkan pembelian dan penjualan produk dan informasi melalui internet dan jasa online lainnya.; (2) digital communications perspective: Sistem yang memungkinkan pengiriman informasi digital produk, jasa dan pembayaran online; (3) service perspective: Sistem yang memungkinkan upaya menekan biaya, menyempurnakan kualitas produk dan informasi instan terkini, dan meningkatkan kecepatan penyampaian jasa; (4) business process perspective: Sistem yang memungkinkan otomatisasi transaksi bisnis dan aliran kerja; dan (5) market-of-one perspective: Sistem yang memungkinkan proses 'Customization' produk dan jasa untuk diadaptasikan pada kebutuhan dan keinginan setiap pelanggan secara efisien. Dengan demikian, pada hakikatnya dalam lingkup yang luas e-commerce bisa dikatakan ekuivalen atau sama dengan e-business.

BEBERAPA ISTILAH DALAM E-COMMERCE

a. **Digital atau electronic cash**: juga dikenal sebagai e-Cash, istilah ini ditujukan untuk beberapa pola/metoda yang memungkinkan seseorang untuk membeli barang atau jasa dengan cara mengirimkan nomor dari satu komputer ke komputer yang lain. Nomor tersebut, seperti yang terdapat di mata uang, diisukan oleh sebuah bank dan merepresentasikan sejumlah uang betulan. Salah satu kelebihan yang dibawa oleh digital cash adalah sifatnya yang anonymous dan dapat di pakai ulang, seperti uang cash biasa. Hal ini merupakan perbedaan utama antara e-Cash dengan transaksi kartu kredit melalui Internet.

b. **Digital money**: adalah terminologi global untuk berbagai e-Cash dan mekanisme pembayaran elektronik di Internet. Yahoo mencatat paling tidak ada 21 perusahaan yang memberikan jasa digital money di Internet.

c. **Disintermediation**: adalah proses untuk memotong jalur perantara. Kira-kira pada saat perusahaan yang berbasiskan web membypass kanal retail tradisional dan menjual secara langsung ke pelanggan / pembeli, maka perantara tradisional (seperti toko dan jasa mail order) akan kehilangan pekerjaan.

d. **Electronic checks**: pada saat ini sedang di uji coba oleh CyberCash http://www.cybercash.com/, sistem check elektronik seperti PayNow akan mengambil uang dari account check di bank pelanggan untuk membayar PAM atau telepon.

e. **Electronic wallet**: Pola pembayaran, seperti CyberCash Internet Wallet http://www.cybercash.com/) akan menyimpan nomor kartu kredit di harddisk dalam bentuk terenkripsi yang aman. Dapat melakukan pembelian-pembelian pada situs Web yang mendukung electronic wallet tersebut. Jika ingin membeli sesuatu pada toko yang mendukung electronic wallet, maka pada saat menekan tombol Pay maka proses pembayaran melalui kartu kredit akan dilakukan transaksinya secara aman oleh server perusahaan electronic wallet. Vendor browser pada saat ini telah berusaha untuk melakukan negosiasi untuk memasukan teknologi e-wallet tadi ke produk mereka.

f. **Extranet**: adalah sebuah kelanjutan dari intranet perusahaan yang mengkaitkan jaringan internal satu perusahaan dengan jaringan internal supplier mereka maupun pelanggan mereka. Dengan cara itu sangat mungkin untuk mengembangkan aplikasi e-Commerce yang memungkinkan menyambungkan semua aspek bisnis, dari proses pemesanan hingga pembayaran.

g. **Micropaymet**: transaksi dalam jumlah kecil antara beberapa ratus rupiah hingga puluhan ribu rupiah, misalnya untuk mengambil / mengakses grafik, game maupun informasi. Pay-as-you-go micropayment seharusnya akan membuat revolusi di dunia e-Commerce. Misal, ESPN SportsZone http://espn.sportszone.com/ menggunakan CyberCoin untuk membayar US$1 untuk mengaskses situs mereka selama satu hari – tanpa perlu membayar penuh langganan bulanan. Kenyataan di lapangan sebagian besar pelanggan yang potensial tidak terlalu bersedia untuk bermain-main dengan micropayment.

h. **B to B e-commerce** : Business to Business e-Commerce adalah perdagangan atau transaksi elektronis yang dilakukan di internet antara pemegang business, baik instansi/lembaga atau perusahaan dengan pihak pemegang business lain baik instansi/lembaga atau perusahaan pula.

i. **B to C e-commerce** : Business to Costumers e-Commerce adalah perdagangan atau transaksi elektronis yang dilakukan di internet antara pemegang business, baik instansi/lembaga atau perusahaan dengan pihak user atau konsumen pemakai jasa internet.

Sistem Pembayaran pada e-Commerce

Untuk pembayaran e-Commerce, ada beberapa altenatif yang disediakan, diantaranya:

1. Melakukan pendaftaran terlebih dahulu sebagai konsumen pada WEB yang terkait. Konsumen yang telah mempunyai kartu kredit dapat menggunakan kartu tersebut untuk pembayaran.

2. Selain kartu kredit, alternatif lainnya adalah dengan menggunakan e-Cash yang merupakan suatu account khusus untuk pembayaran melalui internet. Account tersebut dibuka dengan menggunakan kartu kredit yang dipunyai sebelumnya. Customer hanya perlu mengisi pada account e-cashnya untuk digunakan.

3. Alternatif lain dalam pembayaran di internet adalah dengan menggunakan Smart Card. Di Singapura dikenal dengan istilah Cash Card. Pemakaian Smart Card ini hampir sama dengan pemakaian kartu ATM yang biasa dipakai untuk berbelanja, yaitu pada saat transaksi, uangnya didebet langsung dari account di bank. Untuk pembayaran di internet, user harus memiliki 'Smart Card Reader'. Dalam pemakaiannya, alat khusus ini disambungkan ke port serial di komputer. Pada saat melakukan transaksi, kartu smart card harus digesekkan ke alat tersebut, sehingga chip yang terdapat di kartu dapat dibaca oleh komputer. Untuk softwarenya, yang didigunakan disebut 'e-wallet'. Contoh

web site yang telah menyediakan Smart Card untuk pembayaran adalah http://www.discvault.com.

4. Selain dengan ketiga cara di atas, terdapat alternatif pembayaran yang relatif baru dan belum begitu populer. Alternatif ini adalah penggunaan iCheck, yaitu metode pembayaran dengan menggunakan cek. Pembayaran ini membutuhkan nomor cek milik customer. Web site yang menyediakan penjelasan mengenai cara pembayaran ini adalah http://www.icheck.com.

KEAMAANAN TRANSAKSI ON-LINE

Sama seperti pada dokumen non-elektronik, prosedur keamanan ini akan memberikan manfaat yang besar jika diterapkan dengan benar dan semestinya. Ada dua tingkatan keamanan dalam lingkungan Internet, yaitu:

- Keamanan system (System Security)

  Upaya yang dilakukan untuk menjaga sistem komputer dan dokumentasi serta informasi yang tersimpan dalam sistem baik karena serangan dari luar seperti: password sniffers, masquerading, hacker, cracker, spammer, virus, bencana alam dan sebagainya, maupun serangan dari dalam seperti: pembobolan oleh orang dalam / pegawai. Infrastuktur pendukung keamanan sistem ini antara lain; password, firewall dan value added networks.

- Keamanan Informasi (Information Security).

  Upaya yang dilakukan pada saat informasi elektonik meninggalkan sistem komputer dan tidak ada satupun upaya yang dapat dilakukan oleh sistem keamanan untuk melindungi informasi elektronik itu saat melintasi jaringan atau pada saat berada di komputer lain yang berada di luar jangkauan pengawasan pengirim informasi. Upaya pengamanan informasi saat berada di luar pengawasan pengirim ini menjaga agar tidak terjadi akses tanpa ijin, pembacaan, penggandaan dan pengubahan informasi tersebut dimanapun berada. Ada beberapa cara pengamanan informasi yang dapat digunakan, antara lain: digital signature, timestamping, pihak ketiga yang terpercaya (trusted third party) dan enkripsi.

Kunci dalam semua kegiatan secara online/transaksi elektronik adalah kepercayaan atau trust. Kepercayaan/trust ini akan dimiliki oleh setiap orang atau pihak yang berinteraksi secara online apabila persyaratan hukum dalam komunikasi online (authenticity, integrity, nonrepudiability, writing-signature dan confidentiality) telah dipenuhi. Demikian pula dalam transaksi elektronik, para pihak akan mendapatkan kepastian hukum dan mau berkomunikasi atau melakukan Transaksi elektronik apabila telah memenuhi kelima syarat hukum tersebut. Kelima syarat tersebut dapat dipenuhi apabila keamanan sistem, informasi bahkan hardware terjamin. Isu terpenting dalam transaksi elektronik adalah keamanan. Untuk menjamin keamanan tersebut teknologi telah menciptakan berbagai perangkat yang dapat diandalkan.

Password

Password adalah suatu kata-kata atau karakter rahasia yang mengidentifikasi seorang user untuk mengakses suatu sumber tertentu seperti fasilitas, sistem, dokumen atau rekaman. Password berfungsi seperti kunci. Password digunakan untuk melindungi sistem maupun data dari pihak-pihak yang tidak berwenang untuk mengaksesnya. Sisminbakum telah menggunakan user ID dan password sebagai filter, hal itu benar untuk dilakukan, tetapi kedua hal tersebut bukanlah yang terbaik dan jadi tidak cukup menjamin keamanannya. Ancaman yang terbesar dalam suatu komunikasi online / transaksi elektronik adalah manusia itu sendiri.

Banyak cara yang dapat digunakan untuk mendapatkan password sehingga seseorang dapat memasuki sistem dengan password yang asli, misalnya dengan mengamati password saat diketik oleh user kemudian dihafalkan, atau memanfaatkan kelemahan user yang menuliskan passwordnya di tempat yang tidak aman. Sniffing adalah mengintai dan mengambil password dengan menggunakan program sniffer dimana program ini dapat mengumpulkan 128 bit bahkan 2048 bit pertama setiap sesi dalam jaringan. Perangkat Sniffing dapat menguraikan informasi login dan password. Password yang dibuat kadang terlalu mudah untuk dibongkar, karena user sering memilih password yang mudah ditebak, seperti: tanggal lahir, nama orang terdekat, nama binatang peliharaan, nomor

mobil atau nomor telepon, kata-kata dari kamus, tim olah raga atau artis favorit atau zodiac user.

Password perlu dilengkapi dengan perangkat otentikasi seperti penggunaan smart card, atau perangkat tambahan untuk password seperti password aging, time based password, last login password agar password tidak mudah ditembus. Dengan password yang baik akan dibutuhkan waktu yang cukup lama dan usaha yang cukup keras bagi orang yang hendak membongkar password.

Firewall

Firewall adalah kombinasi dari suatu sistem perangkat keras (hardware) dan perangkat lunak (software) yang dirancang untuk melindungi sistem internal atau jaringan dari dunia luar, misalnya: Internet atau melindungi satu bagian dari suatu jaringan dari yang lainnya. Ancaman dapat datang dari manapun dan serangan yang paling sering dilakukan penyerang adalah berusaha menyusup untuk memperoleh akses ke dalam suatu sistem dengan cara berpura-pura melakukan koneksi dari host yang legal, yang merupakan host target. Penyerang membuat host asli tidak dapat berfungsi dengan melakukan serangan berupa penolakan terhadap servis, selanjutnya penyerang melakukan koneksi ke sistem yang menjadi target dengan menggunakan alamat dari host yang terkena serangan tersebut. Firewall menyeleksi siapa yang boleh masuk ke dalam sistem, komunikasi keluar maupun yang masuk berdasarkan alamat asal, tujuan, port dan tipe informasi yang dikirimkan, firewall ini disebut filtering firewall.

Security Protocols

Sistem pengamanan yang digunakan adalah SSL (Secure Socket Layer). Sistem ini diusulkan oleh Netscape. SSL mengamankan komunikasi Web HTTP antara browser dengan web server. HTTP yang telah aman disebut HTTPS. Dalam SSL ini ada tiga macam protokol pada handshake sequence, yaitu: SSL handshake protocol, SSL change shiper spec protocol, SSL Alert Protocol. Sistem ini mulai bekerja pada sesi SSL dimana browser mengirimkan kunci publik ke server, kemudian server mengirimkan kunci privat ke browser. Browser dan server saling menukar data dengan menggunakan kunci enkripsi rahasia selama sesi tersebut. Sistem pengamanan lainnya adalah dengan menggunakan s-HTTP yang dikembangkan oleh Enterprise Integration Technologies. Perbedaannya dengan HTTPS yaitu adanya sesi protection protocol. Metode lainnya adalah TLS (Transport Layer Security) yang dikembangkan oleh IETF (Internet Engineering Task Force), IPSec (IP Secure) dimana menyediakan servis pada layer 3 dan mengamankan semua yang ada dalam jaringan. IPSec ini didukung oleh Ipv6 yang merupakan generasi IP masa mendatang yang kapasitas alamatnya sebesar 128 bit dan menyediakan jumlah jaringan dan sistem yang tidak terbatas.

Value Added Network (VAN)

Value Added Network (VAN) merupakan suatu perantara komputer jaringan yang menyediakan berbagai pelayanan kepada pelanggannya, termasuk menerjemahkan dokumen-dokumen EDI dalam bentuk yang cocok, menyediakan jaringan yang aman dimana informasi dapat dikirimkan dan penyimpanan rekaman dan fungsi audit.

VAN dimungkinkan untuk meneruskan komunikasi elektronik, yang menggunakan berbagai perangkat keamanan yang dirancang untuk melindungi informasi yang berjalan melalui sistem. VAN juga membatasi penggunaan oleh pemakai dan tidak dibuka kepada umum seperti Internet.· Public Key Infrastructure Sistem pengamanan Informasi yang umum digunakan adalah infrastruktur yang dibentuk oleh sistem kunci publik disebut public key infrastructure (PKI). PKI ini terdiri dari berbagai macam servis yang diperlukan untuk keamanan informasi, seperti: enkripsi, manajemen dan distribusi kunci, digital signature dan certification authority.

Enkripsi

Enkripsi modern mengandalkan algoritma. Dengan menggunakan perangkat lunak (software) atau perangkat keras (hardware) khusus yang bergabung dengan algoritma ini seseorang dapat melakukan enkripsi. Algoritma pun terdiri dari beberapa jenis, yaitu: Data Encryption Standard (DES) dan yang panjangnya hanya 56-bit dan dapat dibongkar oleh cracker dalam waktu kira-kira tiga setengah jam, satu jenis enkripsi lainnya adalah International Data Encryption Algorithm

(IDEA). Seseorang harus juga menyediakan variabel tertentu. Satu variabel merupakan komunikasi itu sendiri, yang merupakan suatu angka binari yang sangat panjang. Satu variabel lainnya adalah kunci yang juga terdiri dari angka yang sangat panjang. Metode enkripsi dibedakan menjadi dua, yaitu: enkripsi simetris dan asimetris.

Dalam metode enkripsi simetris, informasi atau data dalam komunikasi dikunci oleh pengirim maupun dibuka oleh penerima dengan satu jenis kunci yang sama. Berbeda halnya dengan metode enkripsi asimetris dimana terdapat dua jenis kunci yang berbeda untuk mengunci dan membuka pesan yang dikirim. Kunci tersebut disebut kunci publik dan kunci privat. Jenis algoritma dalam metode ini adalah RSA yang diambil dari tiga nama penemunya, yaitu: Rivest, Shamir dan Adelman dan satu jenis lagi adalah Digital Signature Algorithm. Seperti yang telah dijelaskan di atas bahwa terdapat dua jenis kunci dalam metode enkripsi asimetris, yaitu kunci publik dan kunci privat. Kunci publik adalah kunci yang diketahui oleh semua orang, sedangkan kunci privat hanya diketahui oleh orang yang menerima pesan.

Digital Signature

Digital signature dalam definisi teknik adalah suatu tampilan bits yang dihasilkan dengan menggunakan fungsi one-way hash untuk mengacak pesan yang disampaikan dengan komunikasi elektronik sehingga tidak dapat dibaca. Digital signature dibuat dengan cara menggunakan dua kunci sebagaimana diuraikan di atas, kunci publik dan privat. Dalam hal ini penggunaan dua kunci tersebut berbeda dengan metode enkripsi dengan kunci publik. Untuk membuat digital signature digunakan hash function dimana pesan diubah menjadi pesan yang teracak dan tidak dapat dibaca, kemudian pengirim melakukan enkripsi dengan kunci privatnya. Pesan acak yang dienkripsi inilah yang disebut digital signature. Penerima pesan ini harus mengambil kunci publik milik pengirim yang telah ditempatkan di web, smart card, hard disk dan sebagainya, untuk membuka pesan acak tersebut agar dapat dibaca. Proses membuka pesan acak ini disebut dekripsi. Dengan digital signature dan proses enkripsi-dekripsi, terpenuhi lagi dua syarat hukum dalam komunikasi online, yaitu: integrity dan confidentiality. Tanda tangan basah biasanya memiliki ciri nyata yang khusus dan langsung terkait dengan penandatangan.

Berbeda dengan tanda tangan basah, digital signature yang hanya terdiri dari deretan angka-angka yang cukup panjang dimana tidak ada ciri nyata yang khusus dan langsung menujuk kepada penandatangan. Oleh karena itu timbul kesulitan untuk melakukan verifikasi tentang siapa yang memiliki digital signature tersebut. Untuk itu solusinya adalah adanya pihak ketiga yang dipercaya oleh kedua pihak baik pengirim maupun penerima.

Certification Authority (CA) adalah pihak ketiga, baik berupa perorangan maupun badan hukum, yang dipercaya untuk memastikan atau menegaskan identitas seseorang (subscriber), dan bertugas menyatakan bahwa kunci publik dari pasangan kunci publik-privat yang digunakan untuk membuat digital signature adalah milik orang tersebut. CA akan mengeluarkan suatu sertifikat berbasis komputer yang menyatakan hubungan antara suatu kunci publik dan subcriber yang diidentifikasi. Dalam sertifikat tersebut terdapat kunci publik subscriber dan informasi lain yang diperlukan seperti tanggal masa berlakuknya kunci publik.

Untuk menjamin keaslian dan keutuhan isi sertifikat tersebut, CA membubuhkan digital signature CA pada sertifikat. Proses sertifikasi umumnya adalah seperti diuraikan berikut ini : Subscriber membuat pasangan kunci publik dan privatnya; Menemui CA dan memberikan bukti identitas seperti : Surat Izin Mengemudi (SIM), paspor atau bukti identitas lain yang diminta oleh CA; Mendemonstrasikan bahwa subscriber memegang kunci privat yang berhubungan dengan kunci publik (tentunya tanpa membuka/memperlihatkan kunci tersebut); Tahapan proses ini dapat berbeda antara satu CA dengan CA lainnya, misalnya: ada CA yang mewajibkan subcriber datang sendiri menghadap CA untuk memastikan kebenaran identitasnya, namun CA lain bergantung pada pihak ketiga, seperti: notaris untuk memastikan identitas subscriber. CA akan memberitahukan subscriber bahwa sertifikat telah dikeluarkan, hal ini dimaksudkan untuk memberikan kesempatan bagi subscriber untuk memeriksa isi sertifikat tersebut sebelum dipublikasikan. Subscriber diberikan kesempatan untuk memeriksa isi

sertifikat, hal ini penting untuk dilakukan karena Subscriber akan terikat dengan setiap komunikasi yang ditandatangani secara digital dengan kunci privat yang berhubungan dengan kunci publik yang ada pada sertifikat dan bertanggung jawab untuk kesalahan interpretasi dengan CA. Apabila sertifikat tersebut telah diperiksa oleh subscriber dan isinya sudah benar, maka sertifikat itu dapat dipublikasikan oleh subscriber atau meminta CA untuk melakukannya.

Sertifikat dipublikasikan dengan cara direkam dalam satu atau lebih repository / penyimpanan atau disebarkan dengan cara lainnya dengan tujuan agar sertifikat itu dapat diakses oleh setiap orang yang hendak berkomunikasi dengan subscriber. Repository hampir sama dengan yellow pages digital dimana merupakan basis data sertifikat-sertifikat yang dapat diakses online dan dapat diakses oleh siapapun. Repository ini dikelola oleh CA. Guna melindungi para pihak dalam transaksi, maka diperlukan Certification Practice Statements, Certificate Revocation Lists, Certification Expiration, Limits Liability. Timestamping Sebagaimana diketahui bahwa kepercayaan merupakan bagian yang tidak terpisahkan dari Public Key Infrastructure (PKI), namun kepercayaan tersebut harus dapat diverifikasi. Untuk itu digunakan sertifikat digital untuk membuktikan hubungan antara seseorang dengan suatu kunci publik tertentu, dan timestamping memerankan satu peranan pelengkap dan kritis dalam PKI yaitu membuktikan masa berlakunya sertifikat digital dan tanda tangan digital.

Dengan adanya timestamping, dapat diketahui kapan sertifikat digital dibuat, kapan mulai berlaku dan berakhirnya sertifikat. Sebab masa berlaku sertifikat sangat penting artinya. Apabila masa berlaku sertifikat sudah lewat, maka sertifikat tersebut tidak dapat digunakan lagi dalam komunikasi online, dalam arti tidak lagi memberi jaminan dan tidak mengikat bagi para pihak.

E-GOLD

e-Gold adalah suatu alat pembayaran digital baru yang dikeluarkan oleh e-gold Ltd., berkedudukan di Nevis dan berlaku global, dimana standar nilainya didasarkan pada 100% harga emas murni yang berlaku di pasar dunia, dan ditampilkan dalam bentuk rekening tabungan e-Gold. e-Gold merupakan suatu mata uang seperti halnya rupiah dan dollars, namun bukan mata uang nasional suatu Negara tertentu. Nilai transaksinya berdasarkan pada berat emas murni. Dapat merubah e-gold ke dalam bentuk mata uang lain (US Dollars, Pounds, Deutche Mark dan sebaliknya).

E-Gold sudah diakui oleh banyak merchant di seluruh dunia dalam melakukan transaksi on-line, dan sebagai media pembayaran yang sah. Selain itu dana di E-gold dapat ditarik melalui ATM khusus di semua mesin ATM berlogo Cirrus, Maestro, dan Mastercard. Dapat memanfaatkan rekening e-Gold ini untuk menerima pembayaran, melakukan pembayaran, berinvestasi di HYIP. e-Gold memiliki website yang dijamin keamanannya dengan secure server 128 bit SSL. Dapat membuka rekening tanpa dikenakan biaya seperti halnya bila membuka rekening di bank, setelah itu dapat memasukkan dana ke rekening e-Gold dengan cara membeli e-Gold, dan sebaliknya dapat mencairkan dana e-Gold dengan cara menjualnya.

Manfaat E-Gold

Untuk melakukan belanja online (misalnya di : goldstores.com), untuk menyimpan emas secara praktis dan efisien, untuk melakukan pembayaran (e-Commerce, Payrol, membayar tagihan, menyumbang), untuk spekulasi / trading (misalnya di www.gcitrading.com dan di www.betonmarkets.com). Jadi dengan rekening e-Gold ini dapat digunakan untuk menerima pembayaran dan melakukan pembayaran, E-gold memiliki website yang dijamin keamanannya dengan secure server 128 bit SSL.

Dalam membuka rekening e-Gold, tidak dikenakan biaya dan setelah itu dapat memasukkan dana ke rekening dengan cara membeli e-gold atau sebaliknya. Dana pada e-Gold dapat dicairkan dengan cara menjualnya. Transfer antar e-Gold adalah Real Time, artinya dana akan lansung sampai ke rekening tujuan.

Cara Membuka Account e-Gold

1. Klik situs e-Gold pada link **https://www.e-gold.com**

2. Setelah muncul halaman e-Gold, klik **Create Account**
3. Bacalah **User Agreement**, jika setujui klik **I Agree**, kemudian isilah formulir
4. **Account Name**, adalah nama account e-Gold, misal: Uangku1
5. Description boleh diisi boleh juga tidak, kalau diisi maka isilah dengan gambaran diri.
6. **User Name**, isian ini sebaiknya sama dengan Account Name
7. **Alternate Passphrase**, isian ini adalah Password Account e-Gold, diisi dengan gabungan huruf dan angka minimal 6 karakter
8. **New e-Gold Account Passphrase**, sebaiknya sama dengan Alternate Passphrase
9. **New e-gold Account Passphrase Again**, harus sama dengan new e-Gold Account Passphrase. Yang perlu DICATAT adalah passphrase akan selalu digunakan untuk masuk ke dalam Account e-Gold, jadi catat serta jangan sampai lupa dan jangan diberitahukan dengan orang lain. (mirip dengan PIN ATM di bank).
10. **Turing Number Entry**, isilah dengan angka acak yang selalu berubah di sampingnya
11. Klik open
12. Nomor Account e-Gold akan dikirim ke alamat email sesuai yang telah isikan di atas dalam proses isian registrasi
13. Cek email dari e-Gold, catat nomor Rekening e-Gold karena nomor tersebut akan selalu diminta jika mengakses rekening e-Gold.
14. Setelah punya rekening e-Gold, selanjutnya adalah mencoba membuka rekening dengan mengklik link http://www.e-gold.com, klik link Access Your Account
15. Isilah Account dan Passphrases kemudian diikuti Turing Number sesuai nomor yang nampak di sebelah kanan. Nomor ini akan selalu berganti setiap kali mengakses Account. Hal ini dimaksudkan untuk menjaga keamanan dan menghindari pembajakan
16. Selanjutnya jika ingin melihat jumlah saldo uang, klik gambar timbangan (BALANCE). Mengetahui rincian transaksi (print out) silahkan klik HISTORY. Untuk merubah data pribadi, klik ACCOUNT INFO. Mentransfer uang tekan SPEND
17. Jangan lupa, selalu akhiri menekan LOGOUT jika selesai menggunakan rekening.

Mencairkan Dana pada Rekening E-Gold

Untuk mengisi account E-Gold dan juga untuk 'menguangkannya, bisa melakukan' kembali emas, bisa dilakukan melalui jasa para 'merchant' (pedagang). Di situs resmi E-Gold banyak sekali tersedia 'merchant-merchant' ini, dan banyak pula 'merchant' dari Indonesia. Fungsi para 'merchants' tersebut adalah menukar uang dengan emas, dan menukar emas dengan uang (sesuai mata uang rupiah atau yang lainnya).

Beberapa Merchant e-Gold di indonesia dan sekitarnya yang sudah dipercaya adalah:

a. www.greatachiever.com
b. www.plazaegold.com
c. dll

Menjaga Keamanan Rekening e-Gold

Karena e-Gold berisi uang tentunya rentan terhadap pencurian apalagi jika menggunakan fasilitas umum seperti Warnet. Berikut ada beberapa langkah-langkah pengamanan yang dapat digunakan untuk mengamankan rekening e-Gold dari orang yang tidak berhak, yaitu:

1. Pada saat registrasi e-Gold, sebaiknya isi alamat rumah dengan data yang sebenarnya karena apabila lupa password loginnya maka satu-satunya jalan untuk mendapatkan password baru adalah dengan mengirim email ke e-Gold dan e-Gold akan mengirim password baru ke alamat rumah melalui surat/pos (tidak bisa lewat email)
2. Jangan pakai Passphrases e-Gold untuk daftar pada program apapun.
3. Admin e-Gold tidak pernah mengirim email yang ada linknya ke member. Jika ada kiriman email yang meminta mengklik link-nya dan memasukkan Passphrases maka itu adalah hacker yang mempunyai tujuan

mencuri rekening e-Gold dengan membuat WEB mirip dengan situs e-Gold. Untuk itu, abaikan saja atau hapus.

4. Ubahlah password/passphrases secara berkala dan gunakan gabungan huruf dan angka yang sulit ditebak dan lebih dari 10 karakter, gunakan program pengacak misalnya, untuk mengubah password menjadi karakter yang tidak terbaca, rekam password dalam file misalnya untuk kemudian bisa lakukan copy / paste, jika ingin memasukkan password ini (ini jika memakai terminal pribadi)
5. Saat mengisi password/passphrase login, gunakan tombol SRK di kanan isian. Tidak mengetik passwordnya tapi memilih huruf dan angka di window kecil yang muncul menggunakan mouse. Hal ini untuk menghindari password disadap dengan software keylogger yang dapat merekam key yang ditekan. Hati-hati apabila menggunakan komputer public seperti di warnet atau lab komputer, karena bisa saja dipasangi keylogger yang langsung bisa mengirim hasilnya ke email penyadap.
6. Bersihkan selalu komputer yang telah dipakai membuka Account E-Gold sebelum ditinggalkan dengan menghapus semua data yang ada di directory C:\WINDOWS\Cookies, C:\WINDOWS\History dan C:\WINDOWS\Temporary Internet Files
7. Jangan pernah menyimpan data username dan password tersebut pada harddisk komputer meskipun itu komputer pribadi.

KESIMPULAN

Setelah mencermati hal-hal diatas, maka dapat diambil beberapa kesimpulan, yaitu:

1. Dengan menggunakan e-Gold, maka melakukan transaksi melalui internet menjadi lebih aman, karena e-Gold dijamin keamanannya dengan Secure Server 128 bit SSL. Dan hal ini akan membantu pengguna komputer untuk berani menggunakan internet sebagai media untuk melakukan transaksi pembayaran.
2. Sisi keamanan lain dengan menggunakan e-Gold adalah karena pihak yang berhubungan dengan transaksi tersebut tidak mengetahui nomor kartu kredit yang dimiliki (jika melakukan pengisian dana pada Rekening e-Gold dengan menggunakn kartu kredit), sehingga pengguna kartu kredit menjadi lebih aman dari bahaya pencurian nomor kartu kredit.

DAFTAR PUSTAKA

1. http://www.chip.co.id/guides/mencegah-kasus-penipuan-di-ebay-awas-trik-penipu-di-ebay-9.html
2. http://www.e-gold.com
3. http://www.sentraegold.com/enhc/faq_wm_general.php
4. http://www.citywebindo.com/wordpress/?p=13