QUEST

EMPLOYEE ASSISTANCE PROGRAM

Call our toll-free number 1-800-364-6352 for assistance

Worklife Services Newsletter
October 2010

Online Safety

Protecting Your Kids Online

Do you know where your kids are online?

Online pedophiles pretend to be other kids, and cyber stalkers sometimes send kids

threatening or sexually explicit e-mail. Spammers, scammers, criminals and con artists can get names, home addresses, e-mail addresses, Social Security numbers and credit card numbers without the user ever knowing.

When legitimate Web sites for kids started unintentionally contributing to these perils, the government stepped in.

"I think we were all appalled by our naivety when it came to kids' safety online," says John Kamp, a lawyer at the American Association of Advertising Agencies in New York.

It's not a secret that many Web sites collect personal information from their users. Advertisers are trying to find ways to make money on the Web and Web sites want to know how to best serve their customers. But many people worry that data about kids could fall in the wrong hands.

That's where the Children's Online Privacy Protection Act comes in. One of its goals is to let parents know about their children's Web activities. It is also designed to keep kids from the clutches of merciless advertisers, with the ultimate objective of protecting children.

The Federal Trade Commission gave online businesses until April 21, 2000, to change their ways. Kids under 13 can no longer give out any personal information – including e-mail addresses – to commercial Web sites without asking their parents first. And businesses must fess up as to why they want the info.

The law not only affects every child's site such as Disney.com, but every site that collects information from kids simply because it asks for the user's age. Since many kids 12 and younger are already Web-savvy. This law is intended to empower parents and keep kids safe, period. Whether or not it will work remains to be seen.

Making Contracts Online: Electronic Signatures

Electronic contracts and electronic signatures are just as legal and enforceable as traditional paper contracts signed in ink. Federal legislation enacted in 2000, known as the Electronic Signatures in Global and International Commerce Act (ESGICA), removed the uncertainty that previously plagued e-contracts.

This 2000 e-signature law made electronic contracts and signatures as legally valid as

paper contracts, which was great news for companies that conduct business online, particularly companies that provide financial, insurance, and household services to consumers. The law also benefits B2Bs (business-to-business websites) who need enforceable agreements for ordering supplies and services. For all of these companies, the law helps them conduct business entirely on the Internet. This results in substantial savings to businesses, which can be passed on to consumers. For example, one online company estimated that eliminating paperwork fees reduced the cost of processing a home loan by $750.

What Are Electronic Contracts and Electronic Signatures?

An electronic contract is an agreement created and "signed" in electronic form -- in other words, no paper or other hard copies are used. For example, you write a contract on your computer and email it to a business associate, and the business associate emails it back with an electronic signature indicating acceptance. An e-contract can also be in the form of a "Click to Agree" contract, commonly used with downloaded software: The user clicks an "I Agree" button on a page containing the terms of the software license before the transaction can be completed.

Since a traditional ink signature isn't possible on an electronic contract, people use several different ways to indicate their electronic signatures, including typing the signer's name into the signature area, pasting in a scanned version of the signer's signature, clicking an "I Accept" button, or using cryptographic "scrambling" technology.

Though lots of people use the term "digital signature" for any of these methods, it's becoming standard to reserve the term "digital signature" for cryptographic signature methods and to use "electronic signature" for other paperless signature methods.

Cryptographic Signatures (PKI)

Cryptography is the science of securing information. It is most commonly associated with systems that scramble information and then unscramble it. Security experts currently favor the cryptographic signature method known as Public Key Infrastructure (PKI) as the most secure and reliable method of signing contracts online.

PKI uses an algorithm to encrypt online documents so that they will be accessible only to authorized parties. The parties have "keys" to read and sign the document, thus ensuring that no one else will be able to sign fraudulently. Since the passage of the e-signature law in 2000, the use of PKI technology has become more widely accepted. Many online services offer PKI encrypted digital signature systems that function much like we use PINs for our bank cards.

XML-Based Signatures

Other e-signature systems have been developed, including a method for digitally

recording a fingerprint, and hardware that electronically records your signature. In addition, the organization that sets Web standards for the Internet, the Worldwide Web Consortium (W3C), developed XML-compliant guidelines for digital signatures. The results of their working group are discussed at the W3C website at ww.w3.org/Signature.

Opting Out of Electronic Contracts

While the federal e-signature law makes paper unnecessary in many situations, it also gives consumers and businesses the right to continue to use paper where desired. The law provides a means for consumers who prefer paper to opt out of using electronic contracts.

Prior to obtaining a consumer's consent for electronic contracts, a business must provide a notice indicating whether paper contracts are available and informing consumers that if they give their consent to use electronic documents, they can later change their mind and request a paper agreement instead. The notice must also explain what fees or penalties might apply if the company must use paper agreements for the transaction. And the notice must indicate whether the consumer's consent applies only to the particular transaction at hand, or to a larger category of transactions between the business and the consumer -- in other words, whether the business has to get consent to use e-contracts/signatures for each transaction.

A business must also provide a statement outlining the hardware and software requirements to read and save the business's electronic documents. If the hardware or software requirements change, the business must notify consumers of the change and give consumers the option (penalty-free) to revoke their consent to using electronic documents.

Although the e-signature law doesn't force consumers to accept electronic documents from businesses, it poses a potential disadvantage for low-tech citizens by allowing businesses to collect additional fees from those who opt for paper.

Contracts That Must Be on Paper

To protect consumers from potential abuses, electronic versions of the following documents are invalid and unenforceable:

- wills, codicils, and testamentary trusts
- documents relating to adoption, divorce, and other family law matters

- court orders, notices, and other court documents such as pleadings or motions
- notices of cancellation or termination of utility services
- notices of default, repossession, foreclosure, or eviction
- notices of cancellation or termination of health or life insurance benefits
- product recall notices affecting health or safety, and
- documents required by law to accompany the transportation of hazardous materials.

These documents must be provided in traditional paper and ink format.

Consumer Concerns

Although it is expected that secure methods of electronic signatures will be become as commonplace and safe as credit cards, some consumer advocates are concerned that if a consumer uses an unsecure signature method (such as a scanned image of a handwritten signature), identity thieves could intercept it online and use it for fraudulent purposes.

Federal Law Versus State Law

Some states have adopted the Uniform Electronic Transactions Act (UETA), which establishes the legal validity of electronic signatures and contracts in a similar manner as the federal law. If a state has adopted the UETA, or a similar law, the federal electronic signature law won't override the state law. But if a state has adopted a law that is significantly different than the federal law, it will be trumped by the federal law. This ensures that electronic contracts and electronic signatures will be valid in all states, regardless of where the parties live or where the contract is executed.

Government Filings

As for the government, transactions between citizens and the federal government were addressed in 1998's Government Paperwork Elimination Act (GPEA), which created requirements and incentives for the federal government to make electronic versions of their forms available online. A good deal of progress has been made, as many online consumer transactions -- such as paying taxes and registering trademarks -- are now available from the feds. State governments are slowly catching up, as some states now allow you to register your business online.

Password Pointers:

- **Do combine** parts of two unusual, unrelated words, the longer and stranger the better.
- **Do mix** capital and lowercase characters, as well as symbols and numbers, in the middle of the password.
- **Do use** words from a foreign language in combo with an English word. Many hackers try to crack passwords with common words, or with those pooled from the dictionary database of a single language.
- **Don't use** anything that can be easily guessed by people who know you.
- **Don't pair** a common word or your name with a different character at the beginning or end, such as suesmith9.
- **Don't use** the same password from one application to another.