

Security Awareness

Many businesses simply do not include Internet security as part of their day-to-day operations. It is important, though, to develop a 'culture of security.' No matter how good your business procedures, people will make mistakes.

Too many times we forget to log off, do not change passwords, or neglect to download and install the latest software patches. Raising awareness about online security is an important part of protecting your business.

Security Tips

Here are some best practices to remember when online.

- Keep your Operating System patches up to date. Be sure to install all updates,
- Be sure to install all updates to all computer protection tools as well. Install, maintain, and frequently perform scans with your antivirus software, firewalls and email filters.
- Ensure your company's security or IT department runs regular Virus and Malware scans.
- Never install any programs from the Internet if you do not fully trust the source or company providing the software.
- After accessing IRBsearch, please do not leave your computer unattended, without logging out first.
- Also, if enabled, use Ctrl-Alt-Delete on your keyboard when leaving your desk to lock your computer. This ensures that only you will access your systems using your secure password.

That brings us to the next topic of Password Security.

Password Security

Ultimately, you are responsible for securing data and the applications you access on the computer you use. The use of strong passwords acts as a deterrent against password guessing. The security of each individual user is closely related to the security of the whole system. Creating effective passwords can provide additional means of protecting the information on your computer.

Strong Password Tips

Here are some tips for selecting a strong password.

- Never use any easy-to-guess phrases, such as "LetMeIn" or "MyPassword" as your password. Avoid using your birthdate, your child's name, your pet's name, and your spouse's name.
- Don't select a password that a hacker could guess simply by looking around your cubicle or office. Dictionary-proof it: Hackers run "dictionary hacks" in which they check passwords against every word in the dictionary.
- Defeat this attack by using a number or a special character in your password. Be sure to memorize it and never write it down.
- One trick to remembering your strong password is to create a phrase that sticks in your head but is virtually impossible to guess.
- Change your password often especially if you feel someone has seen you type your password or you have mistakenly given it to someone. And lastly,

never give out a password over the phone or email it along with the associated Login ID. You may be thinking, “But what are the chances that I’d give out my password anyway?” Unfortunately, the chances may be greater than you think. And that brings us to our last topic: Phishing.

Phishing

Phishing is a growing Internet scam that uses phony emails to fool people into revealing important personal information such as login IDs, passwords, social security numbers, even credit card numbers.

For example, an email alleging to be from a legitimate source such as IRBsearch.com claims that your account needs to be verified. The email may ask that you go to a website by clicking on a link within the email. When you go to the site, you are asked to "update" or "confirm" personal information such as your login ID and passwords. The website may look just like a legitimate page but is in fact bogus and designed to steal your information.

Tips on How to Avoid Getting Phished

With this in mind, let’s discuss some important practices which will help you avoid becoming the victim of a phisher.

- If you are even remotely suspicious of an email, delete it. When accessing IRBsearch, never click on a link that goes directly to the Login page. Always begin the login process by going to <http://www.irbsearch.com>
- Pay close attention to the URL of a website. Malicious websites may look identical to the legitimate site - graphics and layout are identical - but the URL may use a variation in spelling or a different domain, like .biz vs .com
- When accessing the IRBsearch, verify the correct URL as <http://www.irbsearch.com>. When you click the “Account Login” button, ensure you are being redirected to the correct website by checking the URL.
- Never login by going directly to this page. Always begin the login process by going to <http://www.irbsearch.com>.
- Never reveal personal or financial information in an email and do not respond to email solicitations for this information. This includes following links sent within an email.
- Never send sensitive information over the Internet before checking a website's security. If you are unsure whether an email request is legitimate, verify the request by contacting the company directly.
- However, you don’t want to use the contact information provided in the email or on the website connected to the request. Instead, look up contact information from a more reliable source like a previous statement.
- You can also verify a website by clicking on the padlock icon at the end of the address bar within your browser window.

Also, information about known phishing attacks is available online from groups such as the Anti-Phishing Working Group
http://www.antiphishing.org/phishing_archive.html

As an IRBsearch user, if you ever think or even suspect you have become the victim of a phishing attack change your password immediately. If you have further security questions or concerns, call our Customer Service Department at 800-447-2112. We’re confident that the tips and best practices discussed here will help ensure a safer online experience for you, your business, and ours.