• SECTION ONE – Editorial
• SECTION TWO – Has your email been Spoofed?
• SECTION THREE – Jolene’s Corner
• SECTION FOUR – Risk Perception by Tom Slavin
EDITORIAL

Each year we receive inquiries regarding renewal fees. We try to make it easy to track by including it on the lower right of your certification wallet card that you receive annually. For CSHMs you can also find your COC due date in this same area. We do not want anyone who desires to renew their certification not do so because of a lack of notification. We try to keep current with your contact information and we attempt to keep you informed of the process in the following manner.

**ISHM has two billing cycles for renewal fees.**

If you earn your ASHM or CSHM designation between October 1 and March 30 your renewal cycle will begin on the following October 1. If you earn your ASHM or CSHM designation between April 1 and September 30 your billing cycle will begin on the following April 1.

<table>
<thead>
<tr>
<th>Renewal Date</th>
<th>Invoice Sent</th>
<th>Statement Sent</th>
<th>Statement Sent</th>
<th>Late Fee Added</th>
<th>Statement Sent</th>
<th>Statement Sent</th>
<th>Made Inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>30-Sep</td>
<td>Mid July</td>
<td>August</td>
<td>September</td>
<td>1-Oct</td>
<td>November</td>
<td>December</td>
<td>1-Jan</td>
</tr>
<tr>
<td>30-Mar</td>
<td>Mid Jan</td>
<td>February</td>
<td>March</td>
<td>1 April</td>
<td>May</td>
<td>June</td>
<td>1-Jul</td>
</tr>
</tbody>
</table>
Has your email been Spoofed?

Almost daily we receive email messages from a member’s current email address. It is obvious that the email is not a valid communication and in fact generally contains a link that should you click on will take you to a different commercial site, or worse, invade your computer. These are not nice times in the computer and internet world.

Larry Jaffe, Editor, VIPRESecurityNews, [http://sunbeltsecuritynews.com](http://sunbeltsecuritynews.com) wrote an excellent article on this issue. He graciously allowed me to include it in this newsletter. Please remember this is copyrighted material. We are not endorsing a product, rather we are passing on information we hope you will find useful.

Everything You Wanted to Know about Spoofing but Were Afraid to Ask

**Spoofing:** What Is It? British comedian Arthur Roberts originated the word spoof in 1884 as the title of a game he invented and called Spoof which involved chicanery and deception. The word has come to be defined as a mocking imitation of someone or something, a parody, a host or a prank.

Today in the world of the Internet, it has taken on a more sinister and criminal aspect.

Simply put, email spoofing is the forgery of an email so it appears to be coming from someone other than the actual source. Spammers often use spoofing to get folks to open and potentially respond to their missives. Then there are those unfortunate folks who have seen their email accounts hijacked by hackers and taken over for nefarious purposes.

Email spoofers want you to look at their emails, download malicious software, or click on things you should not be clicking on and taking you places you don't want to go. Unfortunately, it's an increasingly common trick.

**What Can You Do?**

One of the first things you want to do is change your password. But really that is not enough. Here are a few things you need to do to unhijack (is that a word?) your account.

1. As stated change your password. We have written about this numerous times. You can use a password generator like LastPass or RoboForm or you can make up your own strong password or better stated passcode/passphrase. The trick is to create a passcode that is memorable to you yet not easy to crack. First of all don't create one that is less than 8 characters. Use a combination of upper and lower case letters, symbols and numbers. Combine them in a way you will remember but make it strong using the elements indicated above. Oh and do I need to tell you to protect that passcode, don't write it down and paste it to your monitor or something equally dumb.

2. Run a scan with VIPRE to insure there is no malware on your machine sending emails out. There is a chance that your system has been turned into a "spam zombie", where
your system is unwittingly sending out spam emails on behalf of a spammer. That's bad news, but can be fixed by thorough antivirus scanning and cleaning.

3. Don't forget to check your alternative email address! When you sign up for a public email address like Yahoo, Gmail, etc. they ask you for an alternate email address. Don't forget to check yours because a smart hacker might have gone in there and removed yours and replaced it with his own. So make sure you take this extra step.

4. And then there are the secret questions! Another thing email accounts ask for is a secret question like the name of your first grade teacher or first pet. Check to make sure these have not been altered.

5. Mobile or Phone verification: Some accounts ask for your phone number and give you a code to verify your identity. Make sure your phone number has not been changed.

6. Run a scan with VIPRE to insure there is no malware on your machine sending emails out. There is a chance that your system has been turned into a "spam zombie", where your system is unwittingly sending out spam emails on behalf of a spammer. This can be fixed by a thorough antivirus scanning and cleaning.

By carrying out the above five steps, you should be locking out the bad guys who took over your account. Nothing is completely foolproof but this should give you the protection you require. Now, there are the rare cases where your email address has been used in a spam campaign (spoofed to make it look like it came from you), but your account has not been hacked. You'll have changed your password, run a scan with VIPRE and it still continues unabated. The spammer has simply sent an email, but changed the "from" part of the email to your address. What can you do? You'll certainly be getting hundreds, if not thousands, of "bounce-backs" telling you that your email was undelivered to some recipient. In this instance, the only thing to do is to tough it out. It will generally go away after a while, so write a rule in your email program to shovel those bounce back emails into a separate folder and carry on. Like I said, it is rare, but it is known to happen.
**Jolene’s Corner**

In the June I experienced one of the most memorable events of my life and that was traveling to the ASSE Expo in Chicago. With this being my first Health and Safety Expo and the first time ever traveling that far from home, WOW, it had a great impact on me.

I work in the office and work with member names, ID# and with applications and invoices on a daily basis. To travel so far and go to an Expo of that size it was a great feeling to finally see faces that go with the names and numbers. Also it was rewarding to see all the promotions, newsletters and improvement to the website noted and acknowledged.

I also like speaking to others about ISHM and have them tell me that they have heard from a co-worker about us, please tell me more.

With the information and promotions given out at the Expo I eagerly await the replies and applications from those we reached out to.

With that, if you are going to the NSC Expo in Philadelphia in OCT 2011 look for the ISHM booth and come say ‘Hi’ to the staff. We would like to meet you in person.
Risk Perception
Use Lottery Logic
Thomas Slavin CSHM, CIH, CSP

Nature makes us poor judges of risk. We buy lottery tickets and overestimate the chance of winning. Even after several years of losing numbers we still dream about what we will do with the jackpot. We also often underestimate the risk of injury, especially when young as the many daredevil stunts on YouTube show.

Even when we know the odds we often ignore them. Fear of flying may make us drive when statistics tell us driving is much more dangerous. We overestimate the risk of things that we cannot control such as nuclear power or pesticide residues on food, but underestimate the odds when it comes to things that we do control. Common high risk behavior includes such things as not using seat belts, texting while driving, using power tools without safety glasses, using a chair for a ladder, smoking, not using sun screen, not getting medical check-ups, not using a designated driver, not taking medication, listening to loud music or using loud tools (lawn mowers, chain saws) without ear protection. These are well known risks, but we often choose to ignore them.

Sometimes risk is part of the fun, as when people go skydiving or bungee jumping. But more often risky behavior is unintentional. Such perception gaps, when we know the odds but act differently, are the result of mental shortcuts. We do not always have time to make rational decisions; sometimes we just have to react. That can be a good thing when we are being attacked by an animal in the wild, but simply following our impulses can often lead to serious injury.

There are four ways we can manage these unintended perception gaps to improve safety. We can pay better attention to risk. No one ever does something expecting to get hurt. If we knew for sure that our risky behavior would cause an injury we would do things differently. So we could take a second to apply reverse lottery logic and imagine what could happen. Just becoming more aware of risk can improve behavior.

Another thing we can do is develop good habits. Good habits make behavior automatic. Whether it is healthy eating choices, wearing seat belts, pulling over to talk on the cell phone, using ear protection or wearing safety glasses, building a good habit makes it automatic. Every action reinforces the next one. Stopping at a stop sign in the middle of the country when there are no other cars around may seem unnecessary. But if you do not stop you make yourself more likely to blow through the sign when the corn gets taller and there is something coming that you cannot see. If you make a habit of stopping you are more likely to stop when you need to. The most important step is often the very first one.

The third thing to do is set an example for others. It is amazing how much others pay attention to what we do, especially children or grandchildren. One of the best gifts we can ever give to those we love or work with is a good example. If we do not want our children talking on the phone or texting while driving, we should model good behavior and pull over to return calls. If
you do not want to see your coworker hurt, be a model of the good behavior you want them to practice.

The fourth thing is to look out for others. Talking to others about safety is difficult; it is easier with kids but we are uncomfortable telling other adults that they are doing something wrong. Hearing about it is also tough. We do not like to be told what to do and we might not appreciate being reminded that we are taking an unnecessary risk. We need to get comfortable accepting advice and accepting criticism. We also need to say something when we see something. This is the sign of true safety maturity when we are comfortable talking to others about their behavior. Of course, there is a right way and a wrong way to do this. The good way is to explain “you are a good friend and I would hate to see you get hurt; I would feel a lot better if you adjusted the tool rest on that grinder.” One way we can get better at this is to give positive feedback. “I see you are wearing your ear protection. That’s a smart thing to do.” Feedback is a powerful tool that we can use to reinforce good practices.

Nature may be responsible for our perception gaps, but there are ways we can narrow them. Understand yourself better, keep fear in perspective, and make healthier choices for yourself. Above all, develop safe habits and model good behavior for your coworkers and your family. Don’t forget to take safety home.