UTHSC G.U.A.R.D.

November 2017

IN THIS ISSUE

Online Holiday Shopping

by OIT Weekly Newsletter

With the holiday's right around the corner, many of us will begin the task of holiday shopping. As you do so, it is important to be aware that the retail industry is an increasingly attractive target for criminals looking to steal credit card data.

Whether shopping online or in store, it is important that you protect your personal information so that you can avoid being a victim of identity theft. But first, you might ask, "How do I know if my identity has been stolen?" With the increase in retailer data breaches, consumers must take it upon themselves to closely monitor their account activity. The following are some examples of changes that could indicate someone has accessed your information:

- Unusual or unexplainable charges on your bills
- Phone calls or bills from accounts, products, or services that you do not have
- Failure to receive regular bills or mail
- New, strange accounts appearing on your credit report
- Unexpected denial of your credit card

Several habits can help protect you from online identity theft:

- Guard your information online. Never provide your personal information to unsolicited emails and advertisements. Holiday deals may be tempting, but checking the retailer's website first can better protect your information.
- Clear your logins and passwords. This is especially important if you are working on a public or shared computer.
- Pay for online purchases with your credit card, which has better guarantees under federal law then your online payment services or your debit card.
- Always verify that you are on a familiar website with security controls before entering personal data.

For more information, please contact the Information Security Team at itsecurity@uthsc.edu or (901) 448-1880.

Safe holiday shopping online

Read some tips and reminders to stay safe while buying this season

The do's

The don'ts

Think before clicking Send

Review some safety tips about sending and forwarding email messages

A Safety Review of Email Etiquette

by Chris Madeksho, Information Security Coordinator

Email is still one of the primary ways we communicate, both in our personal and professional lives. However, we can become our own worst enemy when using email if we are not careful.

First, let's talk privacy. The traditional email has few privacy precautions. Your email can be read by anyone who gains access to it, unless it is encrypted. (For instructions on email encryption in the UTHSC environment, see October's issue of the GUARD.) Remember that once you send an email, you no longer have control over it. Your email can easily be forwarded to others, posted on public forums, released due to a court order, or distributed if a hacker gains control of your account. If you have something truly private to communicate, pick up the phone.

Second, let's talk about forwarding emails. If you forward an email with an entire conversation attached to it, carefully think if that person receiving your email needs to know everything downstream in that email. Perhaps a summary of what was discussed between the original parties would be better.

Some people like to forward different email addresses into one central address, making it easier to check all different email sources, i.e. work, family, school, etc. Be vigilant about where your emails are forwarded. A hacker that gains access to your account can auto-forward your emails to an outside email address and you might never know it. Periodically check your forwarding rules to make sure your emails are going only where you decide.

Third, let's talk about reply versus reply all. If you get used to using reply all, muscle memory will have you clicking on that option even when you don't want to. Take time to review every email before hitting send.

In the same theme, think about distribution lists. We use them extensively on campus with our listservs. Before sending an email to a group, remember that the message will be sent to everyone in that group. Once it is sent, it is out of your hands and can be forwarded to others outside of your control.

Last, let's talk about auto-complete. It is very easy to start typing out someone's name or email address in the To: field and hitting enter after three letters because that has always been the same person you email consistently. However, lately you have been working with a special group or client with a similar name. All it would take is an unobservant or hurried moment to send sensitive information to unauthorized people.

The best, and most simple advice, is to take a moment before sending each and every email to make sure that you know for certain who is receiving the email and if the subject matter is appropriate for that person or group. For more information, please contact the Information Security Team at itsecurity@uthsc.edu or (901)-448-1880.