Security is everyone’s responsibility. Please read this update carefully, refer to it when needed and ask questions if you need clarification.

Organizations of all sizes face serious challenges with protecting confidential information. As companies continue to expand their use of advanced, secure technologies, hackers and other criminals are attempting to break in organizations by targeting the weakest link: Don’t let it be YOU!

Have you ever received a suspicious phone call, an e-mail from a website, or a text message urging you to click on a link or provide confidential information, such as your credit card number, Social Security number, user IDs and/or passwords? If so, you may have been the target of a phishing attack, “the process used to steal consumer data.” Phishing is a fraudulent attempt, usually made through e-mail, to steal your personal information by masquerading as a trustworthy entity, such as your bank, a retail store or even someone you may know. Phishing is a huge problem and even sophisticated users can fall victim. It can be hard to tell if an e-mail or phone call is legitimate. But don’t despair; here’s help.

WHAT IS A PHISHING ATTACK?

A PHISHING attack generally includes a hook; Trust us. Here’s why, a required action – Here’s what we want you to do, and a push – Hurry, act now! Received emails may state: “During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.”

As users become more familiar with phishing, hackers are launching more sophisticated attacks:

- **Spear Phishing** – often targets specific employees in an attempt to trick them into clicking on a malicious link or an infected attached document.

- **Smishing** – cell phone users receive text messages containing a link to a fraudulent website in an attempt to collect personal information.

- **Vishing** – the voice counterpart to phishing, is the act of using the telephone in an attempt to scam a user into surrendering personal or private information.

Did you know? Legitimate companies will not ask for personal information via e-mail or text.

HOW TO SPOT A PHISH:

Here are some signs:

**Lesson 1:** Be wary of e-mails that play upon emotions designed to provoke a reaction:

- Greed – offering a reward that is too good to be true.
- Curiosity – promises to show something exciting.
- Urgency – indicates a strict “act now” deadline.
- Fear – threatens you with a scare tactic.

**Lesson 2:** Examine e-mail messages closely for:

- E-mail signatures that are overly generic (i.e. from the Billing department),
- Inappropriate message tone for business, or salutations such as “Hello,” or “Greetings, Friend”
- Spelling or grammar errors throughout the message.

**Lesson 3:** Be an Information Security Warrior! Beware of these elements before opening or forwarding e-mails to others:

- E-mail attachments that were not expected or come from someone you don’t know.
- Log-in pages that may steal your personal information or credentials.
- Links that do not match the sender’s name. Always roll your mouse pointer over the link to see if what pops up matches what’s in the e-mail.

When in doubt – STOP, think ... then DELETE! If you are mindful of potential phishing attacks and the tell-tale signs of a scam, you can help minimize your risk of becoming a victim. When it comes to PHISHING, the best line of defense is YOU.
DON’T GET HOOKED:
If you suspect that you have received a suspicious e-mail at work, please forward it to BadEmail@macy's.com or BadEmail@bloomingdales.com. NOTE: These easy to remember email addresses replace the original spoof@macy's.com and spoof@bloomingdales.com addresses.

For more information on Information Security Awareness, check our portal page: http://mymacys.net/sites/mst/infoSec/Pages/Welcome.aspx

IMPORTANCE OF NOT SHARING YOUR NETWORK PASSWORD
You are aware that your network password gives you access to Macy’s, Inc. sensitive information ... but did you know that it also gives access to your personal information in My IN-SITE? This includes your payroll information, health benefits and in some cases, your 401K information, so it’s even more important that you do not share your password.

Sharing your password is against company policy as outlined in the “Policy Regarding Confidentiality and Acceptable Use of Company Systems” located on My IN-SITE/My Policies & Forms/Code of Conduct or on My Macy’s portal under Help & Support/Systems Access. Protect the confidentiality of your password and change it on a regular basis. Keep your password private and safe – NEVER share it.

PASSWORD MANAGEMENT
In these days of hacks and endless breaches, a strong, unique and often-changed password is imperative. Remember:

- NEVER share, reveal or store (unless on an encrypted device) your password.
- Create strong passwords and be creative with special characters, letters and numbers. Mix it up.
- Change passwords IMMEDIATELY if you suspect it’s been compromised.

It’s up to all of us to keep Macy’s, Inc. safe.

Did You Know: Macy’s, Inc. has initiated a new process whereby associates that have registered in the Password Reset Tool will be notified via e-mail every time they change their password? If you have registered via My IN-SITE and receive an e-mail notification but did not initiate a password change, please contact the PC Help Desk at 678-474-2300, option 5 or tieline 8112-474-2300, option 5 to report the issue.

SEE SOMETHING, SAY SOMETHING
Integrity Always, including honest and ethical behavior, is a cornerstone of our business. It’s a value that requires us to do the right thing – always. The Macy’s, Inc. Compliance Connections website enables you to report good faith concerns such as unauthorized access or disclosure of Company business or consumer information, and inappropriate use of systems or passwords. Visit macysscompliancetions.com or call 1-800-763-7290 to learn more.

Remember ... Information security is the responsibility of all Macy’s, Inc. employees.

Please contact the Macy’s, Inc. Help Desk for assistance on PC-related issues including help and support for Bloomingdale’s, macy’s.com, Macy’s stores, Cincinnati and New York Central Offices, Logistics and Operations, Private Brands, Credit and Customer Services, and Systems and Technology.

Direct dial: 678-474-2300 – Tieline: 8112-474-2300

For online assistance, visit the My Macy’s portal Help and Support page: http://mymacys.net/sites/help/Pages/Help%20And%20Support.aspx

ADVICE FOR PROTECTING YOURSELF
As an employee, you have little ability to stop or prevent fraud such as phishing or identity theft. However, there are some positive steps to take to help you become an Information Security Warrior: Always remember the principles of SHRED:

Strong passwords: A strong password should be at least seven characters long and include both capital letters and at least one numeric or other non-alphabetical character. The use of non-dictionary words is recommended.

Handle PII (Personal Identifying Information) with care. Don’t give out personal information on the phone, through the mail or over the Internet unless you initiated the contact or know how it will be used and if it will be shared.

Review your firewall protection software on your home computer. Keep your virus and spyware software programs updated.

Empty your purse or wallet. Don’t carry any more than necessary and never carry your Social Security card.

Discuss these tips with co-workers, family and friends. Share your knowledge and educate those around you.

If you are looking for more information regarding Information Security Awareness, please be sure to check out our portal page at mymacys/sites/enterprise/departments/infoSec/Pages/Welcome.aspx