Holiday Scams

The US Computer Emergency Readiness Team (US-CERT) reminds you to remain vigilant when browsing or shopping online this holiday season. E-cards from unknown senders may contain malicious links. Fake advertisements or shipping notifications may deliver infected attachments. Spoofed email messages and fraudulent posts on social networking sites may request support for phony causes.

To avoid seasonal campaigns that could result in security breaches, identity theft, or financial loss, US-CERT encourages users to take the following actions:

- Avoid following unsolicited links or downloading attachments from unknown sources.
- Be wary of emails or phone calls requesting personal information. Legitimate businesses will not solicit this type of information.
- Check your statements. Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.
- Check privacy policies. Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly.
- Know the seller and the item. Put the company or product name in a search engine, along with “review,” “complaint,” or “scam.” Read the reviews. Be sure you can contact the seller if you have a dispute.
- Avoid clicking links in emails. Scammers know it’s the holiday season. Their phishing scams are after your money or personal information. If an unexpected email promises awesome online deals, don’t click on those embedded links. Check out the company first, confirm its web address, and type it in yourself.
- Pay by credit card. Credit cards give you extra protections, like the right to dispute charges and temporarily withhold payment during an investigation. Whatever the deal might be, never mail cash or wire money to online sellers. And if a company insists you only pay with a gift card, it’s probably a scam.
- Have a safe checkout. Look for a URL that starts with https which indicates that your information is being encrypted during transit. If there’s no ‘s’, if you have doubts, or if you’re asked to email payment info, leave the site.

If you believe you are a victim of a holiday phishing scam or malware campaign, consider the following actions:

- File a complaint with the FBI’s Internet Crime Complaint Center (IC3).
- Report the attack to the police and file a report with the Federal Trade Commission.
- Contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed and do not use that password in the future. Avoid reusing passwords on multiple sites.

Remember, security won’t work without you. YOU are the key to security at PSOM.

Please refer all information security comments or concerns to David Wargo: David.Wargo@uphs.upenn.edu
For more security related information, visit the PMACS Information Security web page: http://www.med.upenn.edu/pmacs/