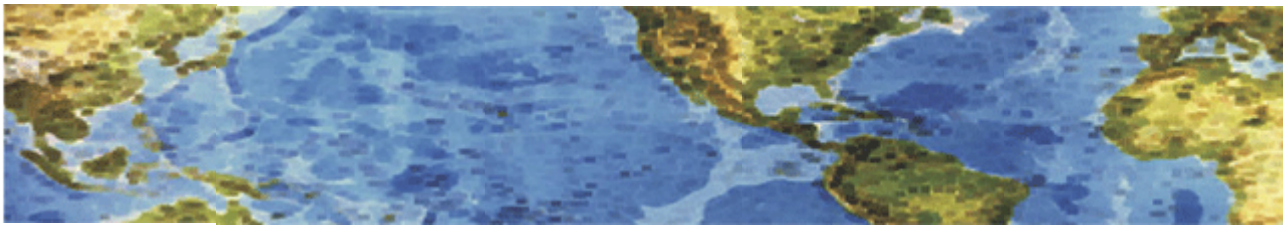
HALL ASSOCIATES



Risk-Based Decision Making Commentary
24 July 2013 Newsletter

Scams about the Royal Baby Lead to Identity Theft

The first celebrity scams about the royal-baby have begun to appear. The first real picture of the royal baby appeared on July 23, and so did the first royal-baby scam. Kaspersky Lab reported on its SecureList blog that an email spam campaign had begun, luring in victims with promises of a hospital webcam. But instead of showing you nurses and infants, the link takes you to a site loaded with the Blackhole browser exploit kit, a particular nasty drive-by download that tries one attack after another against your browser in the expectation that something will get through.

Whenever there's a big news story, scammers and cyberthieves are quick to take advantage of Internet users' curiosity in order to plant malware on their computers, mobile devices and phones and steal sensitive personal information. So be very careful if you're searching for news about the royals or for terms such as "royal baby photos" or "Princess Kate." Online criminals carry out search engine poisoning to turn news-seekers into victims, using marketing techniques to boost phony links to supposedly exclusive items up to the top of Web search results. **But instead of being taken to real news or photos, victims often end up on corrupted or deliberately phony sites that can infect their computers, devices and phones.**

Note that cybercriminals have been preying on celebrity news junkies in the form of phishing emails that promise "exclusive" information about a breaking story ever since the internet began. For example, the royal family has revealed the new prince's birth weight, but that's about all anybody knows so far. The public is clamoring to know the little guy's name, eye color and any other tiny detail. Scammers feed off this hunger and try to get the better of nosy news hounds by emailing to victims messages that claim to have links to secret details about the royal baby. But the recipient will first have to take a survey, log in to Facebook (beware of fake login pages) or provide his name, address and credit-card number.

To avoid falling for attacks such as these, use good anti-virus software and pay attention where online links actually lead. As I've noted before, don't click on any links in email messages you're not expecting and few you are expecting. Stick to major and trusted news sites. If anyone is going to have the latest scoop, it's probably not going to be confined to an obscure and fishy-looking website.

http://www.technewsdaily.com/18579-royal-baby-scams.html?cmpid=529630

HALL ASSOCIATES

Avoiding Online Scams

There are a number of recommendations on how to avoid becoming a victim of an on-line scam. But note that online scams keep changing and becoming more sophisticated. These recommendations are good but will be added to continually.

1. Know who you are dealing with regardless of the type of transaction – find a seller's physical address (not just a P.O. Box) and phone number. Do an internet search for the company name and website and look for negative reviews.

2. Understand that wiring money is like sending cash. It's nearly impossible to reverse such a transaction or trace the money, especially out of the country.

3. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or anyone who claims to be a relative or friend in an emergency who wants to keep the request a secret or for you to respond immediately.

4. Read your monthly statements or check online daily. If you see charges you didn't authorize, contact your bank, card issuer or other creditor immediately.

5. Give only to established charities after a disaster. Don't give to those that have sprung up overnight. For donating tips, check out www.ftc.gov/charityfraud.

6. Don't agree to deposit a check and wire money back. Uncovering a fake check can take weeks and you are responsible for any check you deposit.

7. Don't reply to messages asking for personal or financial information. No government agency or legitimate business will ask for personal or financial information over e-mail, period.

8. Don't play a foreign lottery. Messages saying you have already won are scams. You will most likely be asked to pay "taxes", "fees" or "customs duties" to collect your prize.

Report any online scams – file a complaint with the Federal Trade Commission **(http://www.ftc.gog/complaint)** and your state Attorney General **(http://www.naag.org/current-attorneys-general.php).** For lottery material from a foreign country, give that to your local postmaster. You can also report cyber incidents to the Departtment of Homeland Security:
http://www.dhs.gov/how-do-i/report-cyber-incidents