

## Beware of Holiday Cyber Scams

---

Current smishing schemes involve fraudsters calling victims' cell phones offering to lower the interest rates for credit cards the victims do not even possess. If a victim asserts that they do not own the credit card, the caller hangs up. These fraudsters call from TRAC cell phones that do not have voicemail, or the phone provides a constant busy signal when called, rendering these calls virtually untraceable.

Another scam involves fraudsters directing victims, via e-mail, to a spoofed website. A spoofed website is a fake site that misleads the victim into providing personal information, which is routed to the scammer's computer.

Phishing schemes related to deliveries are also rampant. Legitimate delivery service providers neither e-mail shippers regarding scheduled deliveries nor state when a package is intercepted or being temporarily held. Consequently, e-mails informing of such delivery issues are phishing scams that can lead to personal information breaches and financial losses.

### *Tips*

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail with the link to which you are directed and determine if they match and will lead you to a legitimate site.
- Log directly onto the official website for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
- If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
- Remember if it looks too good to be true, it probably is.