

Cyber Crimes

The unstable economy is creating a large market for cyber criminals. Law enforcement officials who track Internet crime say scams have intensified over the past year, as fraudsters take advantage of the economic anxiety and confusion to target both consumers and businesses. Financial institutions have become the number one target. The latest technique is attacking consumers through their mobile devices.

The scam begins with an innocent text message. The text message appears to come from a legitimate source. The text message may direct the recipient to call a telephone number where an automated attendant prompts them for their account number or their login ID and PIN. The text message may also contain a URL link, leading the recipient to a phishing site. Phishing sites use a criminally fraudulent process in an attempt to acquire sensitive information such as usernames and passwords and credit card details by masquerading as a trustworthy entity.

Until recently, most attacks were random. One text message could be sent to thousands of people. Now scammers are getting smarter. They are doing their homework and targeting specific people or groups of people. This is called spear phishing. Text messages will seem to come from a trusted co-worker or an organization in which the consumer is a member. These messages will come personalized to the individual, addressing them by name, even going as far as referring to the company they work for, or using other personal information they acquire to use against the consumer.

The FBI's Internet Crime Complaint Center confirms an increase in cyber-attacks. The latest statistics reports losses due to cyber scammers to nearly \$265 million. States that have reported text message scams include New York, Pennsylvania and North Dakota.

Here are some tips you can follow that will help you indentify legitimate text messages and those that have malicious intent.

- Never respond to unsolicited text messages
- Never click on a URL in a unsolicited text message
- Always navigate to the website by typing in the address
- Always dial the phone number that you have on file
- Always check credit cards for fraudulent activity
- Always check bank statements for fraudulent activity
- Always report suspicious activity. Reports can be filed at the Internet Crime Compliant Center (IC3) <http://www.ic3.gov/default.aspx>
- Never reveal personal or financial information in a response to a text message, no matter who appears to have sent it



This type of criminal activity will only get more sophisticated with time. The best way to avoid becoming a victim is by educating yourself and Centuric is committed to providing learning resources to consumers through our Centuric Education Center at www.centuric.com.

Centuric specializes in Security for regulated industries and we have partnered with industry leading vendors. We can build a fortress around your company and keep these cyber criminals away. We have proven experience in financial institutions, healthcare, publically traded companies, and large commercial entities.

Contact us today for a **Free Security Evaluation**. We will analyze your technical infrastructure and provide you with an extensive security report.

Call **Now** Toll Free at **866.376.6767**