



2011 IDENTITY THEFT ASSISTANCE CENTER OUTLOOK

WASHINGTON, DC, December 7, 2010--Unemployment, economic uncertainty and the proliferation of technology will be factors in emerging types of fraud over the next year, according to the 2011 [Identity Theft Assistance Center Outlook](#).

“People know they should be skeptical if something appears too good to be true, but in times of stress it’s natural to push caution aside,” said ITAC President Anne Wallace. “The crooks are very good at circumventing our good instincts. Be wary of every communication you receive that asks for information, through any channel.”

Each year ITAC reviews events during the calendar year and surveys law enforcement, researchers and businesses about what we can anticipate over the next 12 months.

New social engineering scams. Criminals used various schemes to exploit consumer fear (*your account has been compromised!*); relationships (*my passport and wallet were stolen, send money please!*) and greed (*you’ve won the lottery!*) over the past year. The Federal Bureau of Investigation’s Internet Crime Complaint Center (IC3) reports a recent sweepstakes scam that sends consumers emails and letters with fraudulent checks bearing the logos of financial services companies. Expect to see variations of these schemes in the coming year using every channel of communication, including text messages and phone calls.

New initiatives to fight fraud and identity theft. In the face of emerging threats, new collaborative projects are supplementing existing public-private partnerships and opening new fronts in the fight against identity theft. “We want consumers to understand that while there may be new scams, financial institutions and law enforcement are working together to curb these threats, and we encourage consumers to join the effort, to be aware, and to be cautious with their information,” said Leigh Williams, President of BITS, the technology policy division of The Financial Services Roundtable.

Williams points to the Financial Services Information Sharing and Analysis Center, which is leading the Account Take Over Task Force, a significant public-private partnership working to protect businesses and consumers from account take over fraud. [Stop. Think. Connect.™](#) is a public education campaign introduced this year and coordinated by the Cyber Security Alliance, whose members include major technology companies and the Department of Homeland security.

The [Identity Theft Council](#) is a new grass roots effort supported by nonprofits and business to recruit volunteers to counsel victims, and provide free training for local police departments.

“The premise of the Identity Theft Council is to help educate consumers about identity theft prevention, and to help alleviate some of the burdens of identity theft cases from resource strapped law enforcement groups,” said Michael Stanfield, CEO Intersections Inc. and co-founder of the ITC.

The wave of cyber crime will not recede. McAfee Labs, which tracks online threats, analyzed and cataloged more threats in the first three quarters of 2011 than in all other years combined and the growth in both volume and sophistication of malware and attacks shows no signs of slowing. Financial institutions also have escalated their efforts to address malware and other attack vectors, and improve the technical and human controls that mitigate these threats.

New forms of small business identity theft. Criminals view small business accounts as a lucrative funding source. The U.S. Postal Inspection Service reports a surge in criminal rings using small business information from stolen mail, check writing software and other tactics to counterfeit checks. They warn business owners not to leave mail unattended: leave it at the post office or give it to a postal employee.

Healthcare reform fraud and medical identity theft. Criminals will exploit fear and uncertainty about the implementation of national health care reform. Earlier this year, Health and Human Services (HHS) Secretary Kathleen Sebelius warned state insurance commissioners about new schemes to sell bogus insurance policies. Medical identity theft – using someone else’s identity to obtain medical services – increased in 2009 and, given high unemployment and the high cost of healthcare – consumers should anticipate seeing more of this crime.

Increase in ATM “skimming.” Security experts report a rise in skimming, a practice that often uses a fake card reader and camera installed on automated teller machines, or wireless technology. There were several skimming attacks in the US and Canada last summer and more attacks that exploit magnetic strip technology are expected.

About ITAC

ITAC, the Identity Theft Assistance Center (www.identitytheftassistance.org), is the national advocate for identity theft victims and a leading voice on identity policy. Millions of consumers have access to the ITAC victim assistance service through our members – the financial services companies who support ITAC and offer it as a free service for their customers. ITAC is dedicated to protecting all consumers through education, research and the criminal prosecution of identity crime. Through our partnership with Intersections Inc, ITAC’s world-class victim assistance and identity management service is available to everyone through ITAC Sentinel® (www.itacsentinel.com).

Media Contact: Kate Ennis (301) 580-6726
kate@enniscommunications.com