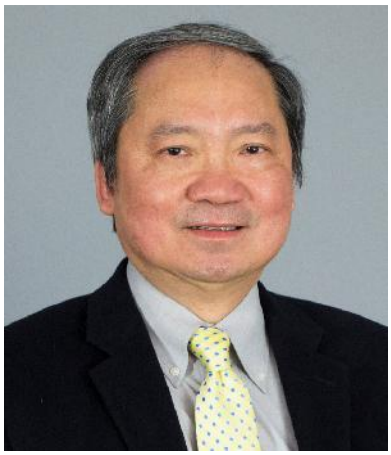
Article 449 May 8, 2016

Banks Work Around the Clock to Thwart Cyber Crooks

By Eddie Ho, Chief Information Officer at Los Alamos National Bank



The Department of Homeland Security in 2004 deemed October as National Cyber Security Awareness Month — a time to raise public consciousness about the ever-more-sophisticated ways in which criminals are trying to steal from working people, businesses and the financial institutions in which they put their money for safekeeping.

But financial institutions think about this problem 365 days a year. Banks invest enormous resources to protect individual and commercial customers from financial security breaches.

Financial institutions have strengthened cybersecurity defenses by embedding chips into credit and debit cards and requiring customers to use two-part authentication to access accounts and bank online. Los Alamos National Bank has used two-factor authentication for all online banking access for many years.

The banking industry must be aware of the next attack method. LANB is connected to major industry security groups — including the Financial Services Information Sharing and Analysis Center, the American Bankers Association, the Department of Homeland Security — and we receive relevant alerts about financial security breaches, allowing us to plan and adjust our controls to prevent a breach. In addition, alerts from payment card channels keep us abreast of new fraud schemes as they're developing.

Participation in information sharing groups such as these allows LANB to be pro-active in defensive controls and fraud management. Passage of the Cybersecurity Sharing Information Act in 2015 means banks and government agencies will collaborate even more to thwart cyber attacks.

Crime-Fighting Partnership

Technology isn't the only solution to combat cyber attacks; banks must invest in qualified staff, cybersecurity training and operating procedures to manage fraud risks effectively. Financial institutions also need customers to help by improving their gatekeeping skills.

Criminals frequently attack financial institutions by going after the customers who can be tricked into dropping their guard. One type of attack, called “social engineering,” manipulates bank account holders into impulsively disclosing confidential information to sources who appear legitimate.

As banks and other financial institutions intensify vigilance about known dangers, crooks will get even more creative about using Web pages and online ads to harvest personal information.

When engaging in financial activities, customers need to be constantly aware of their security environment. They should be suspicious of all communications, including emails, text messages and phone calls. They should configure computer and bank account settings with the maximum security strength available, including the use of multi-factor or two-part authentication when possible. While these tools require customers to keep track of additional passwords, codes and tokens, their use increases account security. Customers should also change passwords frequently and avoid using weak passwords based on birthdays, names of pets and other easily guessed character strings.

Everyone’s Responsibility

Financial institutions and small businesses are usually the ones on the hook when a cyber criminal uses stolen information to buy merchandise under someone else’s name. But customers are harmed when security breaches result in identity theft or make their accounts or funds inaccessible.

Protection of personal information is everyone’s responsibility and customers can play a significant role in avoiding fraudulent transactions by being careful about whom they share information with, following good security practices and avoiding suspicious emails and websites.

Finance New Mexico is a public service initiative to assist individuals and businesses with obtaining skills and funding resources for their business or idea. To learn more, go to www.FinanceNewMexico.org. Sponsored by:

New Mexico Municipal League
NEW MEXICO SBIC
ENCHANTMENT LAND CERTIFIED DEVELOPMENT COMPANY
NEW MEXICO ECONOMIC DEVELOPMENT DEPARTMENT
new mexico MEP manufacturing extension partnership
MONTGOMERY & ANDREWS LAW FIRM
ACCION
WESST
LANB Creating a better way.
The Loan Fund
Los Alamos NATIONAL LABORATORY
LOS ALAMOS National Security, LLC
CENTURYBANK People · Relationships · Community