Safeguarding Association Assets

By: David T. Schwindt, CPA RS PRA

David T. Schwindt

- David T. Schwindt, CPA, a native Oregonian, has over twenty five years experience in public and private accounting including employment with the Portland, Oregon and Denver, Colorado, offices of KPMG Peat Marwick. Mr. Schwindt's tenure was spent primarily in the Private Business Advisory Services Department providing auditing, accounting, tax, and management consulting services for businesses as well as tax compliance and planning for individuals.

- Mr. Schwindt is a graduate of Western Oregon University where he received a Bachelor of Science Degree. He is a Certified Public Accountant in the State of Oregon, Washington, California and Arizona and is a member of the Oregon Society of Certified Public Accountants and the American Institute of Certified Public Accountants. He is a Certified Reserve Specialist – RS, licensed by Community Associations Institute and a Professional Reserve Analyst – PRA, licensed by the Association of Professional Reserve Analysts. He is a past director for Centennial National Bank and Columbine Valley Bank and Trust, Denver, Colorado and member of OWCAM and Oregon CAI LAC. Mr. Schwindt is past President of the Oregon Chapter of Community Associations Institute and was instrumental in organizing the Central Oregon Regional Council.

- Mr. Schwindt specializes in providing accounting, tax and reserve services to Homeowner Associations and currently services over 500 Associations in the Pacific Northwest.

Schwindt & Co.

- Assume everyone wants to steal your money
  - Generally someone you know and trust
- Know who has access to your cash
  - Electronic banking
- Look for incompatible functions
  - (Someone who has access to cash and ability to input accounting transactions)
- Require dual authorizations of expenditures including at least one board member
  - Banks do not look for dual signatures
  - Electronic Banking

Schwindt & Co.

- If bookkeeping is performed by an outside vendor, require a duplicate bank statement be sent to Treasurer
- Read and understand internal financial statements
- Know the difference between a review and audit and limitations of each.
  - Additional audit procedures performed
- Fidelity insurance written by an agent familiar with Associations
- Document and approve the above policies

Schwindt & Co.

Corporate Account Takeover Fraud Headlines…

- N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss
- European Cyber-Gangs Target Small U.S. Firms, Group Says
- E-Banking Bandits Stole $465,000 From California Escrow Firm
- Cyber attackers empty business accounts in minutes
- Zues Hackers Could Steal Corporate Secrets Too
- Computer Crooks Steal $100,000 from Ill. Town
- FBI Investigating Theft of $500,000 from NY School District
- Zues Botnet Thriving Despite Arrests in the US, UK

Schwindt & Co.

CYBER Crime

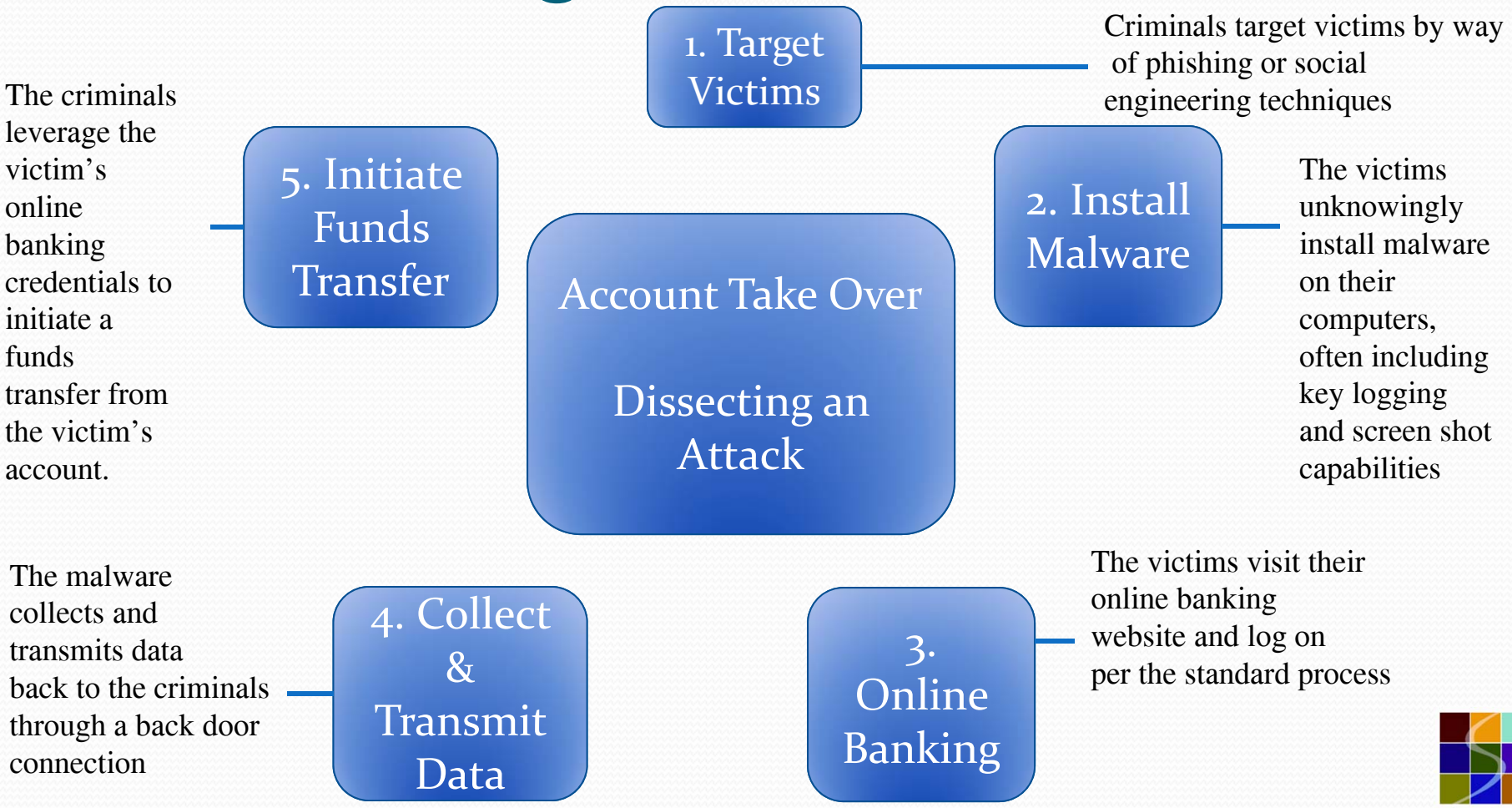
Schwindt & Co.

The Goal of Criminals

- Steal cash
- Steal information that can be converted to cash

Schwindt & Co.

Dissecting a Zues Attack



Schwindt & Co.

Understanding the Adversary

- Known fraud rings are mostly Eastern European (Ukrainian, Russian, Romanian, Estonian) as well as Asian
- Complete service-based economy with specialists in
  - ATMs
  - ACH and wire payment systems
  - Check processing
  - Credit card processing
- Online libraries, education, marketplace and recruitment
  - Malware kits sell for as little as $5,000
  - Some kits even come with tech support
- Attacks involve social engineering and technical aspects
- Project Blitzkrieg – see handout

Schwindt & Co.

Phishing

- Criminals “phish” for victims using emails, pop-up’s and social engineering
- Unsolicited phishing emails may
  - Ask for personal or account information
  - Direct the employee to click on a malicious link
  - Contain attachments that are infected with malware
  - Contain publicly available information to look legitimate
- Phishing emails can be very convincing
  - From UPS: “There is a problem with your shipment.”
  - From your bank: “There is a problem with your bank account.”
  - From the Better Business Bureau: “A complaint has been filed against you.”
  - From a Court: “You’ve been served a subpoena/selected for jury duty.”
  - From NACHA or the Federal Reserve: “Your ACH or wire transaction has been rejected.”
  - From a job applicant: “My resume is attached.”

Schwindt & Co.

Sample Phishing Email

NACHA Phishing Alert (01/19/2010) – Email Claiming to be from NACHA

= = = = = Sample Email = = = = =

Dear bank account holder,

The ACH transaction, recently initiated from your bank account (by you or any other person), was rejected by the Electronic Payments Association.

Please Find Attached Transaction Report

– –

Paul Arnold

Electronic Payments Association Manager

= =

Schwindt & Co.

Malicious Software (Malware)

- Downloaded to PC after employee opens infected attachments in an email or visits a nefarious website
- Newer malware can be acquired *simply by viewing HTML emails*
- Allows criminals to “see” and track employee’s activities internally and on the Internet, including visits to online banking sites
- Criminal uses captured credentials to conduct unauthorized transactions that otherwise appear to be legitimate

Schwindt & Co.

Liability

- Familiarize yourself with your liability for fraud under your financial institution's account agreement
- Losses from Corporate Account Takeover are not covered under Regulation E and, by agreement, are generally the responsibility of the client

Schwindt & Co.

The Key: Protect The End User (and your Association)

Schwindt & Co.

Employee Education

- Alert and aware employees are the best defense
- Hold regular employee education sessions
- Train employees to recognize the threat
- Stay current – read and attend fraud awareness sessions
- Train employees to not open unsolicited emails or click on links
- Contact the “sender” via phone if uncertain as to an email’s authenticity
- Educate Association executives as to the threat and defenses

Schwindt & Co.

Recognize Signs of Malware on the PC

- “System Unavailable” messages while banking online
- Changes in the way your online banking application appears
- Unexpected requests for a one-time password/token in a session
- Unusual pop-up messages
- Computer locks up
- Dramatic loss of PC speed
- Unexpected rebooting or restarting of PC
- New or unexpected toolbars or icons
- Inability to shut down or restart PC
- Warnings from anti-virus or anti-malware software

Schwindt & Co.

Suggestions for Computer Security

- Establish a dedicated computer for online banking
  - Prohibit web browsing, emailing and social networking
- Use anti-virus and anti-spyware technology
- Use secure browser technology
- Do not leave computers unattended or unlocked
- Use spam filters and pop-up blockers
- Install routers and firewalls to prevent unauthorized access
- Do not use public Wi-Fi hotspots such as in cafés and airports

Schwindt & Co.

Suggestions for User Controls

- Require dual authorization to initiate a payment or change administrative rights
  - It's an effective defense to internal *and* external fraud
  - Dual authorization = two users, two PCs and two sets of credentials
  - Apply user and company activity limits
  - Sign up to receive alerts for payments and administrative changes
  - Monitor and reconcile accounts at least once a day
  - Exercise good password management
    - Use strong passwords (mix of letters, numbers, caps and characters)
    - Do not share passwords
    - Different passwords for each online site
    - Regularly change passwords
    - Do not store passwords on your PC

Schwindt & Co.

Suggested Responses to Fraud

- Recognize the signs of malware
- STOP, unplug the machine and contact your bank immediately
- Follow procedures to report suspicious activity at your company
- Ensure your financial institution:
  - Disables online access to your accounts
  - Changes online banking passwords
  - Opens new accounts as appropriate
  - Reviews all recent transactions and cancels unauthorized transactions
  - Looks for new payees, address or phone number changes, new user accounts, changes to existing user accounts, changes to wire/ACH templates, PIN changes, or orders for new checks or other account documents

Schwindt & Co.

Suggested Responses to Fraud

- Document the chronology of the events surrounding the loss
- File a police report; for substantial losses contact the FBI (http://www.fbi.gov/contact-us/field/field-offices)
- Contact your insurance agency
- Have a contingency plan to recover compromised systems
- Contact a forensic IT professional to locate and remove sophisticated malware
- Consider whether other data may have been compromised
- Incorporate “lessons learned” in future employee fraud training

Schwindt & Co.

Summary

- Conduct periodic risk assessments
- Educate employees and executives as to the threat, defenses and risks
- Use a stand-alone PC for online banking; prohibit email, web surfing, etc.
- Use dual control, dual authorization, activity limits, and receive alerts
- Review accounts and transactions regularly
- Recognize the signs of malware on the PC
- Suspect malware? Stop, unplug the PC and contact your FI immediately.
- Comply with the PCI Data Security Standards

Schwindt & Co.

A Classic Risk Management Quote

"*When anyone asks me how I can best describe my experience in nearly 40 years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like. But in all my experience, I have never been in any accident…or any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster or any sort.*"

-Edward J. Smith, 1907

(Captain, RMS Titanic, 1912)

Schwindt & Co.

Sources

- Joint Fraud Advisory for Businesses: Corporate Take Over by USSS, FBI, IC3 and FS-ISAC
- FS ISAC and i-Defense
- 2012 Common Interest Realty Associations Conference Manual
- BB&T Corporation

Schwindt & Co.