Cyber Security Breakout Session

Ed Rosenberg, Vice President & Chief Security Officer, BMO Financial Group
Legal, Corporate & Compliance Group

BMO Financial Group

December 2014

Disclaimer: The material in this presentation provides commonly known information about fraud trends, and BMO's observations about controls and activities. This presentation is intended to provide you and your companies with information and helpful tips, but it does not purport to be complete or provide advice or recommendations to you or your company. You should always seek independent legal or professional advice when implementing fraud or risk initiatives.

Trends in cyber crime

What FIs are seeing today:

- Advanced social engineering techniques
- Targeted spear phishing attacks
- Email takeovers
- Customer/supplier data theft and breaches
- Fictitious identity and impersonation using false or synthetic ID
- Sophisticated Ponzis

Meet the hackers

Organized Crime	Other governments (State sponsored)
Other companies	
Malicious insiders	Careless employees

Means and motives

Why	Market Advantage, Intellectual Property/Corporate Secrets, Revenge, Business disruption, Cyber terrorism, Hactivism
How	Network (Denial of Service, network intrusions); Infrastructure – Servers, desktops, mobile devices; Applications (e.g. website intrusion); Employees (spear phishing)
What	Corporate Secrets, Intellectual property, Business Plans, Identity Information, Strategic & Financial Data; Client information, Access to Accounts
Business Impact	Systems Unavailable, Regulatory sanctions, Litigation, Increased Competition, Revenue Loss; Increased Costs, Reputation Loss; Brand Damage; Loss of Share

Spear phishing

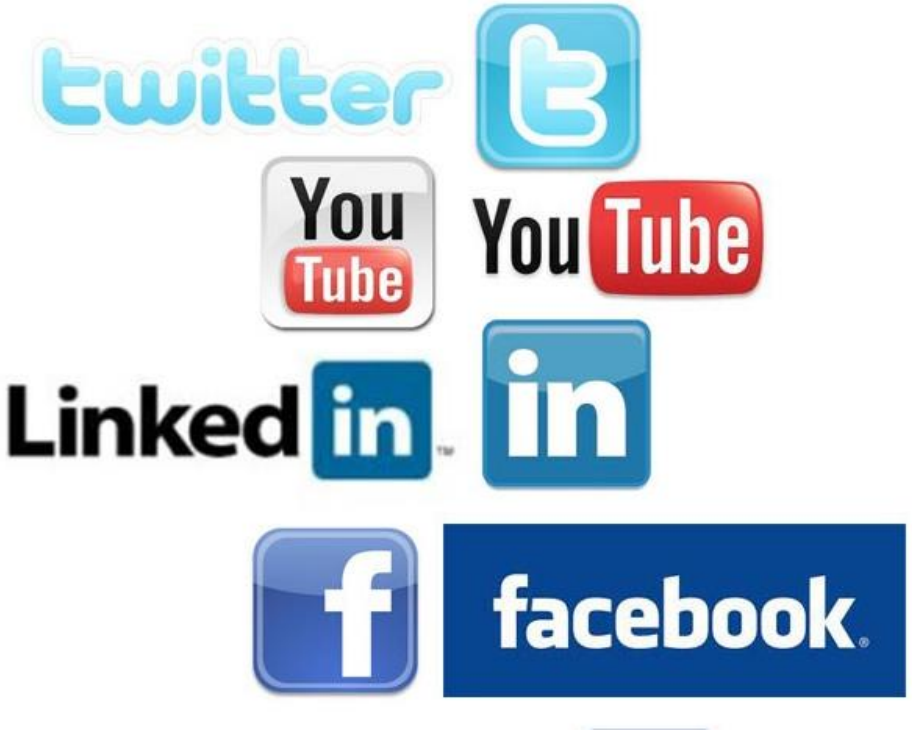
Spear phishing

- One of the best chances of getting access to company networks is through an email spear phishing attack
- Spear phishing is becoming increasingly sophisticated, hard to spot a fake
- Getting into the company's system can also enable email account takeovers and other fraud.

Encryption helps but…

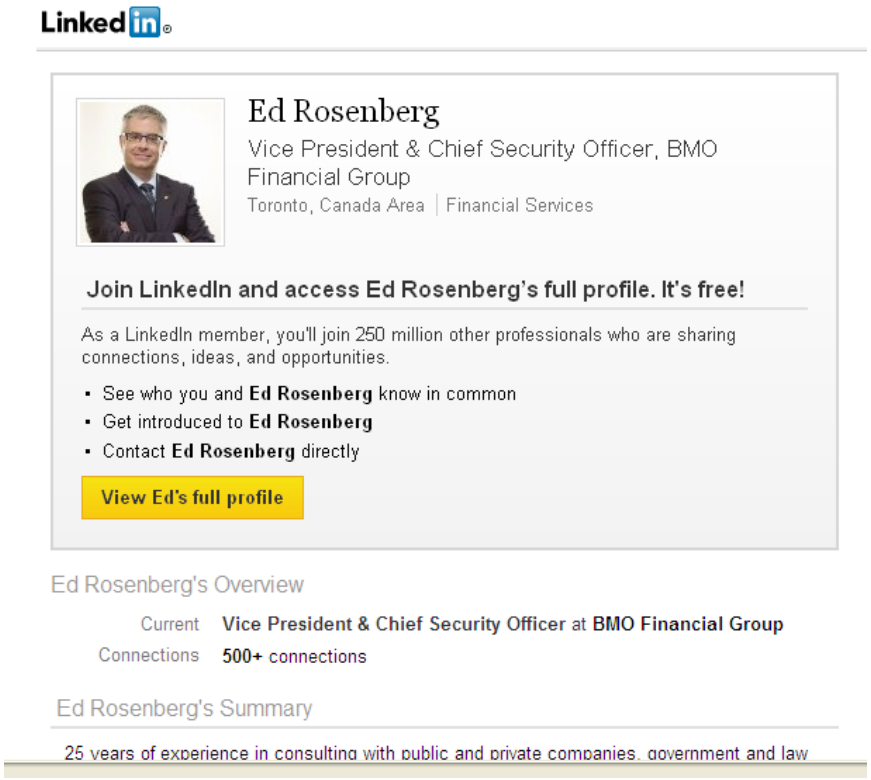
- **Strong encryption** is always a strong defense against hacking – it's difficult to break – but it's not foolproof
- Encryption's weak link: **social engineering.**

Meet the social engineer's New Best Friends



Society for Worldwide Interbank Financial Telecommunication

The increasingly targeted world of social engineering



- **LinkedIn profiles** – critical tool in the social engineer's arsenal
- Targeting certain job profiles in your organization: **Security Analyst, Help Desk Analyst, IT Operations** ⇨ hackers are looking for **Full Admin Rights**
- Titles aid in determining who to target
- Info gleaned from profiles also used to **personalize spear phishing emails** and **hack passwords**.

Email account takeovers

Hacked emails / account takeovers

- Attacks affect more than the user's email account - you can also be a victim if hackers attack:
  - Someone in **your organization**
  - One of your customers
  - Even one of your **suppliers**.

Don't count on noticing anything unusual

- If your own email has been hacked, you might not see unusual traffic or other patterns
  - Hackers can set up filters to forward mail messages to folders (or even to reply and delete before the target sees them).

Ernest E.J. Hilbert, Kroll's 2013/14 Global Fraud Report, p.39

Fraudulent email instructions

How to respond

- Employees who receive email instructions should treat all as fraudulent until the employee can verify directly with the client that the email is legitimate
- Employees need to be cognizant of timing and accuracy when verifying instructions
- In many cases both the fraudster and client are replying from the same email address within the same day (e.g. for wires)

➢ **Best defence against fraudulent emails** is not to accept any instructions through email. Set up phone calls or appointments with the client instead.

Wire payment fraud

Canadian banks and dealers **receive more than 2,000 fraudulent wire instructions a year**

- **Fax, email, telephone** – impostors use different channels
- **Email takeovers** are adding to the problem.

Some ways to mitigate

- Don't accept email instructions
- Segregation of duties (i.e. have a second employee validate client instructions)
- Implement a dollar threshold which would require next level management approval
- Explore monitoring tools (e.g. scrub against set parameters).

Fraud migration: as FIs continue to strengthen fraud detection, fraudsters are now targeting businesses.

Thank you