Victor O. Schinnerer & Company, Inc.

Cyber Risk and Tax Season

How to protect yourself and your clients from booming Social Engineering risks

Cyber Exposures and Tax Season

- Is the risk real?
- What private information is at risk?
- Common/real life examples
- How can I advise my clients to protect themselves and their clients?
- Questions

Is the Risk Real??

- Reports of W-2 Phishing emails increased 870% in 2017 (Per IRS Return Integrity Compliance Services)
- Nearly ONE in FOUR (25%) reported falling for a W-2 phishing email scam
- 76% of organizations reported being victim of a phishing attack in 2016 (Per Wombat Security State of the Phish report)

Is the Risk Real??

- In 2017 and again in 2018, the IRS released YouTube Videos and strongly worded alerts to tax professionals to be on the lookout for email scams
  - IRS, States and Tax Industry Warn Employers to Beware of Form W-2 Scam; Tax Season Could Bring New Surge in Phishing Scheme
  - Phishing Schemes Make IRS 'Dirty Dozen' List of Tax Scams for 2018; Individuals, Businesses, Tax Pros Urged to Remain Vigilant

So, the Risk is Real – but Why?

- Time Sensitivity!
  - A sense of urgency is key for successful phishing scams
- Difficult Topic
  - High reliance on outside professionals = opportunity to exploit trust
- Stressful
  - With time sensitivity and reliance on outside resources – simply seeing email with request for info related to tax filing drives quick review and action
- Constant need for additional information
  - Attachments…click to open and click to “update macros” or similar
  - Additional information requests are expected (and urgent)

What Private Information is at Risk?

- Contact information
  - Success rate for Email from Nigerian Prince vs. corporate accountant…
  - Exploiting “trust”
- Corporate Data/Service:
  - W-2 - This has EVERYTHING needed to file false returns, file for credit, etc.
  - Historical information requests common (and even expected)
  - Benefits, 401K reports
  - Owner tax information tied closely to corporate tax process
- Personal Data:
  - Everything…
    - Any amount, data point, account info – Everything is of value to a scammer

Cyber Insurance Impact

- Tax related information, sensitive financial information well addressed by most all levels of cyber insurance
- Contact information – this is less frequently covered/addressed
  - Note it is specifically contemplated by Schinnerer Cyber Protection Program
- Account history – this is less frequently covered/addressed
  - Note it is specifically contemplated by Schinnerer Cyber Protection Program
- Corporate data/information
  - Many cyber policies do NOT cover third party corporate data!
  - Important item to consider for your Accounting Cyber accounts
  - Note it is specifically contemplated by Schinnerer Cyber Protection Program

Common and Real Life Examples

CEO Scam

- HR contact was tricked into releasing W-2 information on all employees for past year by email purporting to be the CEO of the company

Common and Real Life Examples

AICPA to Accountants

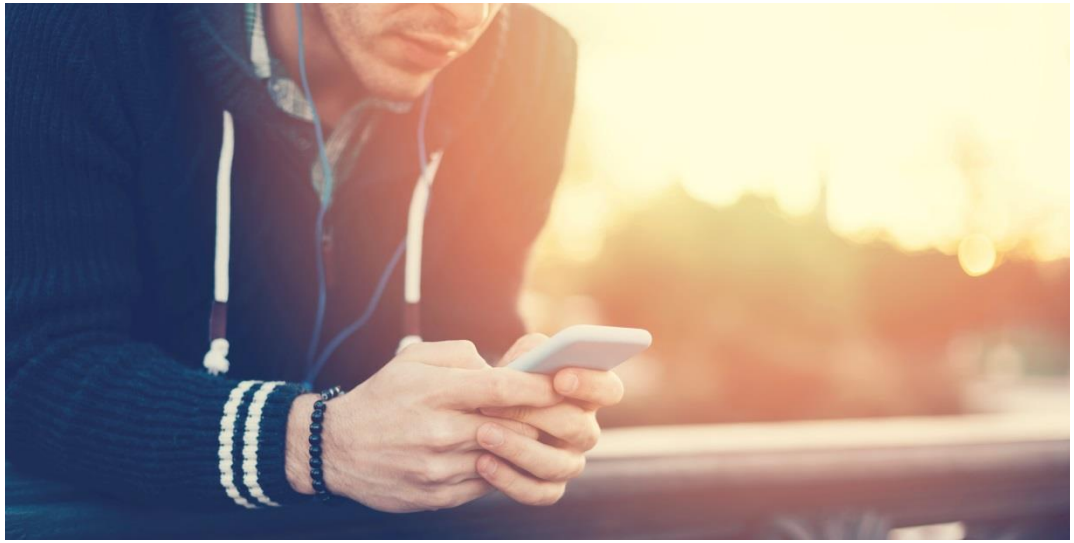
This just happened February 2018!

- Email sent to different state CPA association members
- Email stated something to effect of Termination of Membership and Disciplinary Sanctions levied on the CPA member
- Email contained compromised attachment

Common and Real Life Examples

Emails and Texts and Calls to individuals purporting to be IRS

- Individuals contacted by scammer, often armed with specific information
- Alleging underpayment (or even over-payment) of taxes and seeking either to collect payment or payment info to reimburse
  - Contact info and even single data points can succeed in successful scam or phish



How Can I Advise My Clients to Protect Against the Risk?

- Enable system protections – considerable tools available for enterprises of all shapes/sizes– Microsoft Office 365 has considerable tools including Domain authentication. MimeCast is an advanced email protection software solution
- EDUCATION/AWARENESS – the best software protection in the world can be undone in a second by a user
  - CoFense (fka PhishMe) provides phishing simulation programs to assist in training users to identify phishing messages/attacks
- Educate on sensitivity of the Data shared – Note, this applies to spoken word on the phone, business/personal emails, social network posts…
  - Many would not think verifying a person/business is a client of an Accountant to be sensitive…but it is
- Development/Implementation/Training for understanding of a comprehensive Privacy Policy
  - Risk Based Security – www.riskbasedsecurity.com is good vendor

How Can I Advise My Clients to Protect Against the Risk?

- Enable employees in the process – give them ownership in the responsibility
  - Phish tests, Phish reporting service – www.cofense.com
  - Tax or W-2 related phishing attempts and attacks should be forwarded to phishing@irs.gov
- Training (yes, again and again)
  - Train to analyze whether the information/data is needed by the person asking
    - Does a person on the phone really need the information…
  - Train to identify scenarios that set off alarm bells
    - Email requests with urgency
    - Phone requests with urgency or pressure
  - Train to trust their gut
    - Provide employees a ‘safe’ point of contact to report possible events
    - Support employees reporting the events


Questions?

Contact Me

Jason Bucher
Senior Underwriter
Phone: (913) 685-6166
jason.bucher@schinnerer.com


VICTOR O.
SCHINNERER
& COMPANY, INC.