Tales from the fraud and cyber front at a Maine community bank

Nicole Pellenz
Senior Vice President, Deposit Relationships

Jeremy Clough
Information Security Officer, CISSP CISM CEH CPT
TABLE OF CONTENTS

1. Review of Internet Crime
2. Water Utility Cyber Hygiene
3. Business Email Compromise (Phishing)
4. Payment and Fraud Types
5. Cash Management Solutions to Prevent Fraud
6. What Can You Do?
Internet Based Crime On The Rise

IC3 Complaint Statistics 2014-2018
The Internet Crime Complaint Center (IC3) receives complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.
Internet Based Crime On The Rise
# Internet Based Crime On The Rise

## 2018 Crime Types

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Victims</th>
<th>Crime Type</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>65,116</td>
<td>Other</td>
<td>10,826</td>
</tr>
<tr>
<td>Extortion</td>
<td>51,146</td>
<td>Lottery/Sweepstakes</td>
<td>7,146</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>50,642</td>
<td>Misrepresentation</td>
<td>5,959</td>
</tr>
<tr>
<td>No Lead Value</td>
<td>36,936</td>
<td>Investment</td>
<td>3,693</td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>26,379</td>
<td>Malware/Scareware/Virus</td>
<td>2,811</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>20,373</td>
<td>Corporate Data Breach</td>
<td>2,480</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>18,493</td>
<td>IPR/Copyright and Counterfeit</td>
<td>2,249</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>18,415</td>
<td>Denial of Service/TDoS</td>
<td>1,799</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>16,362</td>
<td>Ransomware</td>
<td>1,493</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>16,128</td>
<td>Crimes Against Children</td>
<td>1,394</td>
</tr>
<tr>
<td>Spoofing</td>
<td>15,569</td>
<td>Re-shipping</td>
<td>907</td>
</tr>
<tr>
<td>Overpayment</td>
<td>15,512</td>
<td>Civil Matter</td>
<td>768</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>15,210</td>
<td>Charity</td>
<td>493</td>
</tr>
<tr>
<td>Employment</td>
<td>14,979</td>
<td>Health Care Related</td>
<td>337</td>
</tr>
<tr>
<td>Tech Support</td>
<td>14,408</td>
<td>Gambling</td>
<td>181</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>11,300</td>
<td>Terrorism</td>
<td>120</td>
</tr>
<tr>
<td>Government Impersonization</td>
<td>10,978</td>
<td>Hacktivist</td>
<td>77</td>
</tr>
<tr>
<td>Rank</td>
<td>State</td>
<td>Victims</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>California</td>
<td>49,031</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Texas</td>
<td>25,589</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Florida</td>
<td>23,984</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>18,124</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Virginia</td>
<td>14,800</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Washington</td>
<td>10,775</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Pennsylvania</td>
<td>10,554</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Illinois</td>
<td>10,087</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Colorado</td>
<td>9,328</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Georgia</td>
<td>9,095</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Maryland</td>
<td>8,777</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>New Jersey</td>
<td>8,440</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Arizona</td>
<td>8,027</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Ohio</td>
<td>7,812</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Michigan</td>
<td>7,533</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>North Carolina</td>
<td>7,523</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Wisconsin</td>
<td>6,621</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Massachusetts</td>
<td>6,173</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Tennessee</td>
<td>5,504</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Missouri</td>
<td>5,508</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Nevada</td>
<td>5,228</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Indiana</td>
<td>4,676</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Alabama</td>
<td>4,585</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Oregon</td>
<td>4,511</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Minnesota</td>
<td>4,304</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>South Carolina</td>
<td>3,575</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Louisiana</td>
<td>3,469</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Connecticut</td>
<td>3,134</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Utah</td>
<td>3,041</td>
<td></td>
</tr>
</tbody>
</table>

**MAINE = 832**
Internet Based Crime On The Rise

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Total Count</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 20</td>
<td>9,129</td>
<td>$12,553,082</td>
</tr>
<tr>
<td>20 - 29</td>
<td>40,924</td>
<td>$134,485,965</td>
</tr>
<tr>
<td>30 - 39</td>
<td>46,342</td>
<td>$305,699,977</td>
</tr>
<tr>
<td>40 - 49</td>
<td>50,545</td>
<td>$405,612,455</td>
</tr>
<tr>
<td>50 - 59</td>
<td>48,642</td>
<td>$494,926,300</td>
</tr>
<tr>
<td>Over 60</td>
<td>62,085</td>
<td>$649,227,724</td>
</tr>
</tbody>
</table>
Water Districts are Targets

- More than a dozen U.S. utilities were directly targeted within the past year (Govtech.com)

- Ransomware is likely your largest threat

- Any water utility that serves more than 3,300 people are now expected to have a risk and resilience assessment completed by June 2021 (EPA.gov)
Utilities Must Stand Up to the Growing Threat of Cyber Crime

By Chris Underhill | May 11, 2016

Our increasing dependence on technology and web-based communication has opened the door for cyber security threats. Cyber criminals are on the increase, and energy and utility companies are high value targets.

Technology and data have completely transformed the power and utilities sector, allowing companies to use information to improve and expand services, and better engage with customers. However, this also brings added regulatory obligations around privacy and security — and the risk that sensitive data will be subject to increasingly sophisticated cyber attacks.

NEWS

Thousands of critical energy and water systems exposed online for anyone to exploit

Critical functions such as starting or stopping a system can be accessed online by anyone, be it nation-state attackers or script kiddies.
Phishing: Don’t Take the Bait

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they’re actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.
Business Email Compromise (BEC)

Beware Unexpected Invoices

AirTemp, Inc.

We are currently upgrading and going digital so all invoices are paid through wire transfers directly to our Finance department.

Sorry for any inconvenience this might cause you, you can set up a wire transfer from your online banking or call your bank and give them our accounting details (see invoice)

Thank you for your business we appreciate it very much

Account department
Business Email Compromise (BEC)

Beware Email Requests to Transfer Funds

From: Ann-Marie Evans  
Sent: Monday, January 28, 2019 10:04 AM  
To:  
Subject: Loon Pt Closing Docs

Morning,
I have received the closing docs. Please ensure payment goes to our Bank of America account.
Let me know once payment is completed.

Thank you,

Ann-Marie Evans
Processor
Machias Title
33 Broadway Suite 3
Machias, ME 04654
Phone: (207) 779-9191
Fax: (207) 255-6640
Business Email Compromise (BEC)

Beware Email Requests to Transfer Funds

Ann-Marie Evans annmarie@machiaastitle.com

Ann-Marie Evans annmarie@rnachiaastitle.com
Business Email Compromise (BEC)

Beware Requests Involving Gift Cards

From: Miranda Smith Machias <f@earthlink.net>
Sent: Monday, June 10, 2019 8:46 AM
To: xxxxxxx

Okay, I'm in the middle of something now. I need physical eBay gift cards, purchased, can you make this happen? If so, let me know if you can quickly please.

Sent from my iPhone

-----Original Message-----
From: xxxxxxx
Sent: Jun 10, 2019 5:44 AM
To: Miranda Smith Machias
Subject: RE: Re:

Good morning Miranda,

Of course how can I help?

Thank you,

From: Miranda Smith Machias
Sent: Monday, June 10, 2019 8:40 AM
To: xxxxxxx
Subject: Re:

Got a moment? I need you to complete a task for me.

Sent from my iPhone
Business Email Compromise (BEC)

Beware Requests To Open Shared Documents
Malware Infection via Attachments or Advertisements

Don’t click on unexpected link or attachments

Sent: Monday, May 20, 2019 2:55 PM
Subject: SUSPICIOUS WEBLINK: Wegerer Melissa has shared a file with you via OneDrive

Please find attached.

OneDrive Attachments
May 21 2019
Expires

SKM_15512294597860 1.5MB

Download Attachment

STOP | THINK | CONNECT

Machias Savings Bank
Microsoft, Apple or any reputable company will never contact you via phone, or with a popup, to warn you that your PC is infected and needs support to run better.

Brian Krebs’ Three Rules of Online Security:

1: If you didn’t go looking for it, don’t install it.

2: If you installed it, update it.

3: If you no longer need it (or, if it’s become too big of a security risk) get rid of it.
During 2018, the FBI received 1,493 complaints regarding ransomware infections, a number smaller than the 1,783 from 2017 and 2,673 complaints it received in 2016, and the 2,453 received in 2015. Ransom paid was $3,621,857 in 2018.
Phishing Email Demonstration
Best Phishing Defense
WannaCry: 2017 Ransomware

- Exploited Known NSA Vulnerability (MS17-010)
- Developed by North Korean Military Lazarus Group
- $100,000 in ransom collected
- 200,000 machines infected
- Kill Switch identified and enabled by security researcher
- Ransom notes utilized Google Translate:
  “But you have not so enough time”
Cryptocurrency Mining

Tech support fraud saw a 90% increase in losses from 2016 to 2017.
Phishing Defense: Education

Hey!

Is this your car? The headlights were left on. I thought you would like to know!

Sent from mobile device
ah ha, I can see right through you scam email stupid

On Wed, Mar 20, 2019 at 9:56 AM &lt;Clough@machiasavings.com&gt; wrote:

Jeremy Clough
Information Security Officer
p. (207)643-5945 m. (207)749-9499

Voted One of the Top Banks to Work For in the Nation – American Banker Magazine
From: &lt;Jeremy3501@machiasavings.com &lt;Jeremy3501@machiasavings.com&gt;
Sent: Wednesday, March 20, 2019 9:04 AM
To: Clough, Jeremy &lt;Clough@machiasavings.com&gt;
Subject:

The information contained in this email message from M3B may be privileged, confidential, proprietary, or otherwise protected from disclosure. If you have received this email in error, please notify us immediately by replying to the message and please delete the message from your computer. Thank you, M3B

Adam
Fundamentals

- Perform Asset Inventories
- Assess Risks
- Minimize Control System Exposure
- Enforce User Access Controls
- Safeguard from Unauthorized Physical Access
- Install Independent Cyber-Physical Safety Systems
- Embrace Vulnerability Management
- Create a Cybersecurity Culture
Fundamentals

- Develop and Enforce Cybersecurity Policies and Procedures
- Implement Threat Detection and Monitoring
- Plan for Incidents, Emergencies, and Disasters
- Tackle Insider Threats
- Secure the Supply Chain
- Address All Smart Devices (IoT, IIoT, Mobile, etc.)
- Participate in Information Sharing and Collaboration Communities
Manage Payables

97%
Manage Payables

- WHY use electronic services?
  - Simplify payroll and expense reimbursement
  - Pay employees quickly and predictably
  - Provide direct deposit services for employees and vendors
Electronic Payment Benefits

- Cost savings: 47%
- Fraud control: 42%
- Better supplier/customer relations: 38%
- Speed of settlement: 37%
- More efficient reconciliation: 35%
- Improved cash forecasting: 32%
- Straight-through processing to A/P or A/R: 27%
- Ability to take early payment discounts: 23%
- Working capital improvement: 17%
- Reduction in days sales outstanding (DSO): 7%
- Client retention: 6%

Source: 2019 AFP® Electronic Payments Survey | www.AFPonline.org
Trends in noncash payments

Card payments have grown significantly over the past decade

Payment volume: number of payments by payment type (billions)

- Credit cards
- Debit Cards
- Checks
- ACH

*The Federal Reserve’s estimates for ACH and check payments are only available through 2015

Source: Federal Reserve
Trends in noncash payments

Check payments have declined substantially in recent years

Payment volume: annual growth rate in number of payments by payment type

- Credit cards
- Debit Cards
- Checks
- ACH

2012-2015
- Credit cards: 8.0%
- Debit Cards: 7.5%
- Checks: -3.0%

2015-2016
- Credit cards: 10.4%
- Debit Cards: 6.5%
- Checks: 5.3%

2016-2017
- Credit cards: 9.4%
- Debit Cards: 10.4%
- Checks: -4.8%

*2015-2016 and 2016-2017 estimates for checks and ACH are based on information from the largest depository institutions

Source: Federal Reserve
Types of Payments Fraud

- Check Fraud
  - Altered
  - Counterfeit
  - Remote Deposit Capture (RDC)

- Electronic Fraud (ACH & Wire)
  - Corporate Account Takeover
  - Social Engineering

- Credit Card / Debit Card / Purchasing Card

Source: 2019 AFP® Payments Fraud and Control Survey
Check Fraud

NAME & ADDRESS

ROUTING & ACCOUNT #
Check Fraud

Business Checking Accounts
Use your US based business checking account. Learn more

Add a business checking account

Where are my account numbers?

Name on Account

Bank Routing Number

Account Number

Re-enter Account Number

Business Tax ID
Enter your business’s 9-digit Employer Identification Number (EIN). Sole proprietor? Enter your Social Security Number instead.
Wires

Wires – Second to checks

Trends in Payments Fraud Activity
(Percent of Organizations that Experienced Attempted and/or Actual Payments Fraud)

#1 CHECKS

#2 WIRES
Automated Clearing House

- Expedite payment collection and processing
- Control transaction settlement dates to optimize cash flow
- Decrease NSF/returned item fees
- Lower processing costs vs. checks
- Reduced exposure to check fraud
- Simplify payroll, tax and vendor payments
- Flexible
Protection

Consumer Financial Protection Bureau

Master
Check Positive Pay

- Compares checks presented for payment to issued-check files
  - serial numbers
  - dollar amounts

- Payee validation and payee match identifies payee names that have been altered

- Reverse positive pay (alternative)
  - companies unable to transmit check files

- Approve or decline items within certain timeframes
ACH Positive Pay

- Blocks and Authorizations
  - accept transactions from authorized suppliers (automatically)
  - return unauthorized incoming debits or credits

- Approve or decline items within certain timeframes
Establish Payment Protocols

- Physical or Electronic Forms for Payment (BILLS)
- Payment Limits
- Bank Controls
- Employee Education
- Written Policies
- Internal & External Audits
- Segregation of Duties
What Can You Do?

Protect yourself.

» Keep your computer security up to date and back up your data often.

» Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.

» Change any compromised passwords right away and don’t use them for any other accounts.
Phishing

Avoid the Hook

Check it out.
» Look up the website or phone number for the company or person who’s contacting you.
» Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
» Tell them about the message you got.
Two Factor Authentication

Your Phone <> Your Identity

(But it is still much, much better than nothing!)
Cyber Security Program

- Review and Update Policies
- Utilize dual-control whenever possible
- Identify Devices and Data Locations
- Perform Risk Assessments
- Patch and Track Vulnerabilities
- Review Network Activity
- Educate About Phishing and Malware
- Encourage Incident Reporting
- Carefully Review Vendors
- Test Incident Scenarios
**Step 1: Backup your files regularly:** Use a cloud service and an external drive you disconnect from the PC.

**Step 2: Keep your PC clean:** Always make sure that you have a real-time antivirus program running on your PC, and make sure this program is always up-to-date. Spectrum and Comcast both offer free anti-virus with most of their offerings.

**Step 3: Enter Safe Mode:** Before you do anything, you need to disconnect your PC from the internet, and don’t use it until you’re ready to clean your PC.

**Step 4: Delete temporary files**

**Step 5: Run scan for malware (anti-virus and malware bytes)**

**Step 6: Check your web browser:** Before launching your web browser, check your homepage and connection settings. Simply go to the settings window of your browser to check your homepage setting.

**Step 7: Recover your files if Windows is corrupt:** If you can’t seem to remove the malware or if Windows isn’t working properly, you may have to reinstall Windows. But before wiping your hard drive, copy all of your files to an external USB or flash drive.

**Step 8: Bring your PC to a PC shop for a professional cleaning/re-image**
RESOURCES

Water ISAC https://www.waterisac.org/fundamentals

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) – www.ic3.gov

SANS Security Insights – www.sans.org

NEACH – www.neach.org

National Cyber Security Alliance (NCSA) – www.us-cert.gov
(Department of Homeland Security)

Government Finance Officers Association (GFOA) – www.gfoa.org
Filing a Complaint with IC3

- Victim’s name, address, telephone and email address
- Financial transaction information (e.g. account information, transaction date, amount and who received the money)
- Subject’s name, address, telephone, email, website and IP address
- Specific details regarding the event
- Email header(s)
- Any other relevant information to support the complaint

www.ic3.gov
“Usually I don’t kill the messenger, but you used PowerPoint.”
Discussion