Tales from the cyber front at a community bank in Maine

Jeremy Clough
Information Security Officer
CISSP CISM CEH CPT
Internet Based Crime On The Rise
Internet Based Crime On The Rise

Brewer School Department pays $1,400 in ‘ransom’ to unlock computer system

Cyberattack hits Augusta municipal operations; City Center closed

Officials say a nasty, intentionally deployed virus shut down public safety computers and made the city’s entire network unusable, but the phone system and public safety radio system were not affected.

July 31, 2019

Cyberattack forces Houston County schools to postpone opening day

Several thousand school children in Alabama had their summer vacation extended by two weeks as the Houston County School District was forced for the second time to delay opening day due to a cyberattack.

Houston County Schools Superintendent David Sewell told families the first day of school will now be August 12, instead of the originally scheduled Aug. 1, according to a WTVY report. Initially, Sewell had pushed the start back from August 1 to August 5, but this required an additional adjustment.
# 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 Impersonation</td>
<td>10,978</td>
<td>Hacktivist</td>
<td>77</td>
</tr>
</tbody>
</table>
Internet Based Crime On The Rise

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Victims</th>
<th>Rank</th>
<th>State</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>49,031</td>
<td>30</td>
<td>Kentucky</td>
<td>2,813</td>
</tr>
<tr>
<td>2</td>
<td>Texas</td>
<td>25,589</td>
<td>31</td>
<td>Oklahoma</td>
<td>2,644</td>
</tr>
<tr>
<td>3</td>
<td>Florida</td>
<td>23,984</td>
<td>32</td>
<td>New Mexico</td>
<td>2,127</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>18,124</td>
<td>33</td>
<td>Kansas</td>
<td>2,098</td>
</tr>
<tr>
<td>5</td>
<td>Virginia</td>
<td>14,800</td>
<td>34</td>
<td>Iowa</td>
<td>1,983</td>
</tr>
<tr>
<td>6</td>
<td>Washington</td>
<td>10,775</td>
<td>35</td>
<td>Mississippi</td>
<td>1,882</td>
</tr>
<tr>
<td>7</td>
<td>Pennsylvania</td>
<td>10,554</td>
<td>36</td>
<td>Arkansas</td>
<td>1,849</td>
</tr>
<tr>
<td>8</td>
<td>Illinois</td>
<td>10,087</td>
<td>37</td>
<td>Alaska</td>
<td>1,603</td>
</tr>
<tr>
<td>9</td>
<td>Colorado</td>
<td>9,328</td>
<td>38</td>
<td>Idaho</td>
<td>1,513</td>
</tr>
<tr>
<td>10</td>
<td>Georgia</td>
<td>9,095</td>
<td>39</td>
<td>District of Columbia</td>
<td>1,364</td>
</tr>
<tr>
<td>11</td>
<td>Maryland</td>
<td>8,777</td>
<td>40</td>
<td>Nebraska</td>
<td>1,205</td>
</tr>
<tr>
<td>12</td>
<td>New Jersey</td>
<td>8,440</td>
<td>41</td>
<td>West Virginia</td>
<td>1,109</td>
</tr>
<tr>
<td>13</td>
<td>Arizona</td>
<td>8,027</td>
<td>42</td>
<td>Hawaii</td>
<td>1,100</td>
</tr>
<tr>
<td>14</td>
<td>Ohio</td>
<td>7,812</td>
<td>43</td>
<td>New Hampshire</td>
<td>1,056</td>
</tr>
<tr>
<td>15</td>
<td>Michigan</td>
<td>7,533</td>
<td>44</td>
<td>Rhode Island</td>
<td>1,028</td>
</tr>
<tr>
<td>16</td>
<td>North Carolina</td>
<td>7,523</td>
<td>45</td>
<td>Delaware</td>
<td>897</td>
</tr>
<tr>
<td>17</td>
<td>Wisconsin</td>
<td>6,621</td>
<td>46</td>
<td>Maine</td>
<td>832</td>
</tr>
<tr>
<td>18</td>
<td>Massachusetts</td>
<td>6,173</td>
<td>47</td>
<td>Montana</td>
<td>787</td>
</tr>
<tr>
<td>19</td>
<td>Tennessee</td>
<td>5,584</td>
<td>48</td>
<td>Puerto Rico</td>
<td>704</td>
</tr>
<tr>
<td>20</td>
<td>Missouri</td>
<td>5,508</td>
<td>49</td>
<td>Vermont</td>
<td>525</td>
</tr>
<tr>
<td>21</td>
<td>Nevada</td>
<td>5,228</td>
<td>50</td>
<td>Wyoming</td>
<td>497</td>
</tr>
<tr>
<td>22</td>
<td>Indiana</td>
<td>4,676</td>
<td>51</td>
<td>South Dakota</td>
<td>465</td>
</tr>
<tr>
<td>23</td>
<td>Alabama</td>
<td>4,585</td>
<td>52</td>
<td>North Dakota</td>
<td>459</td>
</tr>
<tr>
<td>24</td>
<td>Oregon</td>
<td>4,511</td>
<td>53</td>
<td>U.S. Virgin Islands</td>
<td>65</td>
</tr>
<tr>
<td>25</td>
<td>Minnesota</td>
<td>4,304</td>
<td>54</td>
<td>Guam</td>
<td>52</td>
</tr>
<tr>
<td>26</td>
<td>South Carolina</td>
<td>3,575</td>
<td>55</td>
<td>U.S. Minor Outlying Islands</td>
<td>47</td>
</tr>
<tr>
<td>27</td>
<td>Louisiana</td>
<td>3,469</td>
<td>56</td>
<td>American Samoa</td>
<td>16</td>
</tr>
<tr>
<td>28</td>
<td>Connecticut</td>
<td>3,134</td>
<td>57</td>
<td>Northern Marina Islands</td>
<td>15</td>
</tr>
</tbody>
</table>
Internet Based Crime On The Rise

2018 VICTIMS BY AGE GROUP

<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>
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

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
To: [Redacted]
Subject: Loan Pt. Closing Docs

Monday, January 28, 2019 10:04 AM

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,
/AM
Business Email Compromise (BEC)
Beware Email Requests to Transfer Funds

Ann-Marie  amarie@machiastitle.com
Ann-Marie  amarie@rnachiastilltitle.com
Experienced people. Exceptional service

Business Email Compromise (BEC)
Beware Requests Involving Gift Cards

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

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 stop by the nearest store so I can advise the quantity and domination to procure. You can turn in the expense report when you are done with the purchase later.

Sent from my iPhone

-----Original Message-----
From: xooooxxx
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: xooooxxx
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
Romance Scams and Online Predators
Malware Infection via Attachments or Advertisements

Don’t click on unexpected link or attachments

From: 
Sent: Monday, May 20, 2019 2:55 PM
Subject: SUSPICIOUS WEBLINK: [redacted] has shared a file with you via OneDrive

Please find attached.

OneDrive Attachments
May 22 2019

SKM_15512294597860
1.5MB

Download Attachment

STOP | THINK | CONNECT™

Experienced people. Exceptional service
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.

Tech support fraud saw a 90% increase in losses from 2016 to 2017.

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.
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

Experienced people. Exceptional service
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.
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.
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.
Two Factor Authentication

Your Phone <-> Your Identity

(But it is still much, much better than nothing!)
Enroll and Monitor

28 Plant Your Flag, Mark Your Territory

Many people, particularly older folks, proudly declare they avoid using the Web to manage various accounts tied to their personal and financial data — including everything from utilities and mobile phones to retirement benefits and online banking services. The reasoning behind this strategy is as simple as it is alluring: What’s not put online can’t be hacked. But increasingly, adherents to this mantra are finding out the hard way that if you don’t plant your flag online, fraudsters and identity thieves may do it for you.

The crux of the problem is that while most types of customer accounts these days can be managed online, the process of tying one’s account number to a specific email address and/or mobile device typically involves supplying personal data that can easily be found or purchased online — such as Social Security numbers, birthdays and addresses.
Cyber Security Program

- Review and Update Policies
- 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
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 9:16 AM <Jeremy.Clough@machiasavings.com> wrote:

Jeremy Clough
Information Security Officer
p. (207)501-3945 m. (207)749-9493
Voted One of the Top Banks to Work For in the Nation-American Banker Magazine

Sent: Wednesday, March 20, 2019 9:36 AM
To: Clough, Jeremy <Jeremy.Clough@machiasavings.com>
Subject: ______________________

TASKalfa 3501i
[00:17:24:55:15]

MSBMallGate.MachiasSavings.com made the following annotations

The information contained in e-mail messages from MS 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, MSB
How Can You Help?

• Talk with your students about basic cyber hygiene

• Test students and staff with phishing emails (yup, really!!!!)

• If you don’t have two factor authentication in place for your school email, (nicely) ask why

• Ask Administrators and IT support if you have Cyber Incident Response Plans in place
PC Infected?

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
Discussion