Item No. 12
Town of Atherton

CITY COUNCIL STAFF REPORT – REGULAR AGENDA

TO: **HONORABLE MAYOR AND CITY COUNCIL**
GEORGE RODERICKS, CITY MANAGER

FROM: **ANTHONY SUBER, DEPUTY CITY MANAGER / CITY CLERK**

DATE: **DECEMBER 16, 2020**

SUBJECT: **REVIEW AND APPROVE THE RESPONSE TO GRAND JURY REPORT: "RANSOMEWARE: IT IS NOT ENOUGH TO THINK YOU ARE PROTECTED"**

RECOMMENDATION

Review and approve the attached response to the San Mateo County Grand Jury Report on their report entitled "Ransomware: It Is Not Enough To Think You Are Protected".

BACKGROUND

The Superior Court of California, of the County of San Mateo Grand Jury filed a report on October 7, 2020 entitled "Ransomware: It Is Not Enough To Think You Are Protected" which contained findings and recommendations pertaining to cities in San Mateo County. The intent of the report was to present best practices in developing Cybersecurity strategies and provide recommendations for agencies to evaluate. California Penal Code Section 933.05 requires any agency that is the subject of such a report to reply in writing at a public meeting. The response is due to the Grand Jury no later than January 5, 2021. The City Clerk / Deputy City Manager prepared the attached reply to the Grand Jury Report for Council consideration and approval as Attachment 1.

FINDINGS | ANALYSIS

The summary provided by the Grand Jury Report indicated a December 2019 online survey sent to all 68 public entities in San Mateo County with a 54% response rate (37 survey responses and 1 verbal response). The survey concluded that over 25% (10 of 38) of the public entities indicated they had been a victim of one or more Ransomware attacks. A component of the report recommends developing, implementing, and testing a Cybersecurity strategy for each jurisdiction. The report outlined suggested steps agencies should consider improving for defenses, ability to detect incursions, and ability to respond to Ransome attacks. Those steps include:

- Using firewalls to protect internal environments from breaches;

- Using malware detection software to monitor incoming emails and network activity;
- Ensuring that users are educated and tested to learn what to watch for an avoid, especially in emails;
- Developing and fully testing a thorough backup and restore strategy to enable a complete recovery from an attack;
- Putting in place internal controls such as subnets, which require departmental authorization to access other department's data or programs.

The Town's Information Technology (IT) Department (via consultant contract with Interwest Consulting Group) maintains a Ransomware Recovery Plan that was updated in November 2020 and a Cybersecurity strategy. The strategy is intentionally not overly detailed with possible system weaknesses in order to maintain a high degree of confidentiality. The Town provides cyber security training to all staff annually. The training presentation and cyber security tips provided to staff in February 2020 is included as Attachment 3. The report identifies several exposure areas of ransomware and other malware attacks for local public entities, listing *phishing* as the single largest exposure threat. The Town has taken steps to impede and limit this risk including branding incoming email messages with an advisory warning that notes the email comes from an external source and heading caution in opening attachments or links from unknow or suspicious origins. This represents one of the mitigating strategies used to limit the risk of exposure.

The 2019-2020 Grand Jury report recommendations require the Town to report on of the following actions for each recommendation:

1. The recommendation has been implemented, with a summary regarding the implemented action
2. The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.
3. The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of publication of the Grand Jury report.
4. The recommendation will not be implemented because it is not warranted or reasonable, with an explanation, therefore.

One of the survey questions asked what defenses were currently employed to block malware and a list of best practices for those defenses was included in the report. They include:

- Filtering incoming email for viruses, malware, and phishing attempts;
- Utilizing protection software from multiple vendors;
- Utilizing multiple layers of defense;
- Keeping systems up-to date.

The Grand Jury Report recommends regular reviews of Cybersecurity strategies, employee trainings, and testing defense strategies. The report concludes with a comprehensive list of best

practices from professional literature and Information Technology Managers that have successfully defended attacks:

- Anti-Malware definitions need to be constantly updated to retain their effectiveness.
- Software updates need to be kept current
- To identify external emails, message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content.
- To thwart phishing attempts, footers can be added to incoming emails to warn about opening attachments and clicking on links.
- Security training, awareness and assessment need to be routine along with testing all employees to recognize, delete and report attempted attacks
- Establishing a thorough and comprehensive backup process for all Servers using the 3-2-1 rule and establishing a separate backup process for key users' critical folders (e.g., administration, accounting, human resources) to be able to restore/recover from a secure onsite and/or offsite backup.
- Snapshots and/or image backups provide the most complete backup and the fastest recovery option.
- Consider cloud-hosting of email and other applications to provide added security, backup & restore capabilities and filtering benefits to close the largest and easiest route for Ransomware to penetrate entity systems.

Within the report are eight (8) Findings:

1. Ransomware is a real and growing threat to public entities including those in San Mateo County.
2. Across the country, local governments and schools represent 12% of all Ransomware attacks.
3. The direct and indirect costs of Ransomware can be significant.
4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.
8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

The Report concludes with four (4) Recommendations to which each jurisdiction must respond.

1) Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a

report from their IT organization that addresses the concerns identified in the report, specifically:

a. System Security (Firewalls, Anti-malware/ Antivirus software, use of subnets, strong password policies, updating/patching regularly)

b. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)

c. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

2) These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

3) Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

4) Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool.

As stated, the Report is intended to present best practices in developing plans and strategies. It provides information to be discussed related to potential concerns and recommends IT staff confidentially and urgently assess their respective Ransomware protection strategies.

POLICY FOCUS

The Grand Jury requires that the Town respond to the findings and recommendations in the report. Staff has provided responses for the City Council's consideration. Staff has agreed with all findings and provided responses on the recommendations.

FISCAL IMPACT

None.

COMMISSION/COMMITTEE FEEDBACK/REFERRAL

This item ____ has or __X___ has not been before a Town Committee or Commission.

____ Audit/Finance Committee (meets every other month)
____ Bicycle/Pedestrian Committee (meets as needed)

____ Civic Center Advisory Committee (meets as needed)
____ Environmental Programs Committee (meets every other month)
____ Park and Recreation Committee (meets each month)
____ Planning Commission (meets each month)
____ Rail Committee (meets every other month)
____ Transportation Committee (meets every other month)
____ Tree Committee (meets each month)

ATTACHMENT

1. Attachment 1 - Response to Grand Jury Report
2. Attachment 2 - 2019-2020 San Mateo County Grand Jury Report "Ransomware: It Is Not Enough To Think You Are Protected"
3. Cybersecurity Training Presentation

TOWN OF ATHERTON

ADMINISTRATIVE OFFICES
150 WATKINS AVENUE
ATHERTON, CALIFORNIA 94027
(650) 752-0500

December 17, 2020

Hon. Danny Y. Chou
Judge of Superior Court
C/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655

SUBJECT: RESPONSE TO GRAND JURY REPORT: "Ransomware: It Is Not Enough To Think You Are Protected"

Honorable Judge Chou,

Attached please find the Town of Atherton's response to the above Grand Jury Report. The response to both the findings and recommendations are listed below. Pursuant to California Penal Code Section 933.05, the response was considered by the City Council at a public meeting on December 16, 2020.

Should you have any questions concerning the response, please contact City Manager George Rodericks at (650) 752-0504 or grodericks@ci.atherton.ca.us.

Respectfully,

TOWN OF ATHERTON

Mayor

Response to Grand Jury Report Findings and Recommendations

Report Title: “Ransomware: It Is Not Enough To Think You Are Protected"

Report Date: October 7, 2020

Response by: Town of Atherton

From: , Mayor

The Town of Atherton is responding to each Finding solely with respect to itself and not regarding any other City.

Response to Grand Jury Findings:

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County. Response: The Town of Atherton agrees with this finding

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks. Response: The Town of Atherton agrees with this finding

F3. The direct and indirect costs of Ransomware can be significant. Response: The Town of Atherton agrees with this finding.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.
Response: The Town of Atherton agrees with this finding.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.
Response: The Town of Atherton agrees with this finding.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.
Response: The Town of Atherton agrees with this finding.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity’s backup plan to recover lost information.
Response: The Town of Atherton agrees with this finding.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.
Response: The Town of Atherton agrees with this finding.

Response to Grand Jury Recommendations:

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F,

should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:
1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)
3. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

Response: This recommendation has been implemented
The Town of Atherton City Manager's Office made this request of the Town's IT Department upon receipt of the Grand Jury Report. The IT Department will prepare a study session report for City Council which will, at a minimum, address the concerns listed in R1.1, R1.2, and R1.3.

R2. These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

Response: This recommendation will be implemented by the June deadline
The Town of Atherton's IT Department will prepare a comprehensive study session report for City Council, planned for Q1 calendar year 2021, that addresses the concerns identified in the report. This report will include actions taken and plans for future enhancements.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security and/or a cyber hygiene assessment from the County Controller's Office.

Response: This recommendation will be implemented on or before June 30, 2021
The Town of Atherton IT Department will make a request with the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, for cyber-hygiene services before June 30, 2021.

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

Response: This recommendation will be implemented on or before June 30, 2021

The Town of Atherton IT Department will utilize the Federal Communications Commission Cyber Security Planning Guide and the FCC Cyber Security Planner to review and update our cyber-security plans. This work will be completed on or before June 30, 2021.

Superior Court of California, County of San Mateo
Hall of Justice and Records
400 County Center
Redwood City, CA 94063-1655

NEAL TANIGUCHI
COURT EXECUTIVE
OFFICER
CLERK & JURY
COMMISSIONER

(650) 261-5066
FAX (650) 261-5147
www.sanmateocourt.org

Town of Atherton
City Clerk Department

OCT 13 2020

RECEIVED

October 7, 2020

Councilmember
Town of Atherton
91 Ashfield Road
Atherton, CA 94027

Re: Grand Jury Report: "Ransomware: It Is Not Enough To Think You Are Protected"

Dear Councilmembers:

The 2019-2020 Grand Jury filed a report on October 7, 2020 which contains findings and recommendations pertaining to your agency. Your agency must submit comments, within 90 days, to the Hon. Danny Y. Chou. Your agency's response is due no later than January 5, 2021. **Please note that the response should indicate that it was approved by your governing body at a public meeting.**

For all findings, your responding agency shall indicate one of the following:

1. The respondent agrees with the finding.

2. The respondent disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons therefore.

Additionally, as to each Grand Jury recommendation, your responding agency shall report one of the following actions:

1. The recommendation has been implemented, with a summary regarding the implemented action.

2. The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.

3. The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of publication of the Grand Jury report.

4. The recommendation will not be implemented because it is not warranted or reasonable, with an explanation therefore.

Please submit your responses in all of the following ways:

1. **Responses to be placed on file with the Clerk of the Court by the Court Executive Office.**

   - **Prepare original on your agency's letterhead, indicate the date of the public meeting that your governing body approved the response address and mail to Judge Chou.**

Hon. Danny Y. Chou
Judge of the Superior Court
c/o Jenarda Dubois
Hall of Justice
400 County Center; 8th Floor
Redwood City, CA 94063-1655.

2. **Responses to be placed at the Grand Jury website.**

   - **Copy response and send by e-mail to: grandjury@sanmateocourt.org. (Insert agency name if it is not indicated at the top of your response.)**

3. **Responses to be placed with the clerk of your agency.**

   - **File a copy of the response directly with the clerk of your agency. Do not send this copy to the Court.**

For up to 45 days after the end of the term, the foreperson and the foreperson's designees are available to clarify the recommendations of the report. To reach the foreperson, please call the Grand Jury Clerk at (650) 261-5066.

If you have any questions regarding these procedures, please do not hesitate to contact Paul Okada, Chief Deputy County Counsel, at (650) 363-4761.

Very truly yours,

Neal Taniguchi
Court Executive Officer

Enclosure

cc: Hon. Danny Y. Chou
Paul Okada

Information Copy: City Manager

Ransomware:
It Is Not Enough To Think You Are Protected

ISSUE

City and county government computer systems are at risk of Ransomware attacks. Are adequate measures being taken by local government agencies to mitigate the risks and provide recovery options?

SUMMARY

Ransomware has already hit many governmental Information Technology (IT) systems in San Mateo County. In December 2019 the Grand Jury sent an online survey to all 68 public entities in San Mateo County,[1] received 37 survey responses (a 54% response rate), and interviewed several responders including one IT Manager (who had refused to respond to the survey for fear of being successfully attacked once again), for a total of 38 responses via survey and interview. More than 25% (10 of 38) of the public entities responding to the Grand Jury reported that they have been a victim of one or more Ransomware attacks. More concerning is the certainty that there will be more attempts to violate the integrity of our local governments' electronic infrastructure.

This report is intended to present "best practices" in developing a Cybersecurity strategy, then implementing and testing that plan. It addresses actions that can be taken (and have been taken, in some cases) in order to guard against Ransomware attacks, recover from an attack and the additional measures that can be taken to reduce the possibility of an attack. However, it is not an exposé with details of potential system weaknesses, in light of the need for Cybersecurity strategies and practices to be highly confidential. As such, this report walks the line between providing an informed discussion of potential concerns without providing a road map of how to breach public government IT systems.

The single largest exposure every organization has to cyber-thieves is phishing, the illegal practice of sending legitimate-looking emails to an organization's employees. These emails may contain malware or links that, when clicked, infect the computer with a virus that can spread to the entire information systems network.

Although many email software programs include some level of protection against Ransomware attacks, such protections require customization and activation, and it is not clear that local public entity IT departments are undertaking these necessary customization and activation steps. In addition, training for new employees and recurring training for existing employees is critical to dramatically reducing the probability of a Ransomware infection. In some agencies, it appears

[1] See Appendix F: Public Entities in San Mateo County (Cities, County, School Districts, Special Districts)

that only limited training is provided for new employees with little or no recurring training provided for current employees.[2]

Ransomware and other malware attacks are a test to an organization's backup and restoration procedures.[3] The Grand Jury found that none of the survey responders has actually performed a full restore as a test of their backup process. However, without adequate testing, backups do not provide sufficient protection.

Rigorous preparation for an attack is essential if fast and full recovery is desired and the payment of a ransom is to be avoided. There are several significant steps that local public entities should take to improve their defenses, their ability to detect incursions, and their responses to Ransomware attacks. These steps include:

- Using firewalls to protect internal environments from breaches;
- Using malware detection software to monitor incoming emails and network activity;
- Ensuring that users are educated and tested to learn what to watch for and avoid, especially in emails;
- Developing and fully testing a thorough backup and restore strategy to enable a complete recovery from an attack;
- Putting in place internal controls such as subnets, which require departmental authorization to access other department's data or programs.

In addition, cloud hosting should be considered for email and certain applications to reduce the success of Malware and Ransomware attacks on information systems infrastructure.

While all attacks are malicious in terms of time and potential data loss, in the case of Ransomware (or worse, Ransomware 2.0 that also infects backup data) the financial cost of paying the ransom in order to remove the infection and restore a data system can be significant. Alternatively, if the decision is to not pay the ransom but to attempt to recover from the infection manually, the direct and indirect costs could be considerably more.

This report is directed to the governing bodies of government entities in San Mateo County urging them to have their IT staff confidentially and urgently assess their respective Ransomware protection strategies and training and then move with all deliberate speed to address any shortcomings in their Cybersecurity programs.

GLOSSARY

CLOUD COMPUTING
Cloud computing is the delivery of on-demand computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis. Rather than owning their own computing infrastructure or data centers, companies can rent access to

---

[2] Grand Jury interviews

[3] Epicor Corporation, *Protecting Yourself From Ransomware*, January 2020

anything from applications to storage from a cloud service provider.[4] Some examples of this are Yahoo Mail, services like Google Docs, and customer relationship management software.[5]

CYBERSECURITY
Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.[6] Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and recovery.

ENCRYPTION
The process of locking out the contents of a file and the renaming of the file such that it cannot be opened and used in the intended application (e.g. Microsoft Excel). Typically, a 128 Bit (or larger) encryption key (a long series of letters and numbers) is used first to encrypt then later to un-encrypt a file.

MALWARE
Short for "malicious software," this software is designed specifically to damage or disrupt computer systems. Not all malware is Ransomware because some malware has no related attempt to extort money.

PHISHING
The illegal practice of sending email claiming to be from reputable companies to induce individuals to reveal personal information or click on website links or open attachments that then install malware.

RANSOMWARE
Ransomware can be simply described as an infection on a host machine that prevents access to data until a ransom is paid. The most common method of infection is to encrypt files making them totally unreadable by a user. The infection is usually delivered by a *Trojan Horse* (a term referring to the misleading of users of its true intent) installed when a user clicks on a malicious link or attachment in an email.

RANSOMWARE 2.0
This newer version of Ransomware no longer is just malware that encrypts data and asks for ransom, the attacker also threatens to release the data onto the internet and demands money in order not to do so. This newer Ransomware works in such a way that even backup copies of most important files will not be able to save an infected organization.[7] By planting the malware but delaying its activation, Ransomware 2.0 can infect backups thus defeating their value.

---

4 https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

5 Pearson Education, Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, page 655

6 https://digitalguardian.com/blog/what-cyber-security

7 https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

BACKGROUND

Ransomware is a real and serious threat to every entity: government organizations, corporations, and individuals. The more dependence an organization has on the software and data in its network(s), the more important the concern should be. Loss of access to mission-critical data, systems, and software can severely impact an organization in both the short and long term.

According to an October 2019 report by the National League of Cities, since 2013, Ransomware attacks have been reported by at least 170 county, city or state government entities across the United States.[8] The actual number is likely to be much higher because it represents only those attacks that have been reported. Many infections go unreported when ransoms are paid,[9] when organizations are seeking to avoid embarrassment, or when the attacks were simply undetected or untraceable.[10] This has been true even in San Mateo County where local public governing entities have had Ransomware attacks that were not publicly reported.[11]

Not only do such data breaches embarrass and slow organizational productivity, they can be very expensive. For example, the MIT Technical Review (2019) asserts: "Ransomware may have cost the U.S. more than $7.5 billion in 2019… the victims were 113 governments and agencies, 764 health-care providers, and up to 1,233 individual schools affected by Ransomware attacks…most local governments do a poor job of practicing Cybersecurity."[12] The cost to the city of Atlanta to recover from its Ransomware breach was estimated at $17 million.[13] Similarly, a recent Baltimore Ransomware breach is estimated to have cost over $18 million.[14] In 2020, the UC San Francisco School of Medicine paid $1.14 million in ransom to recover its own data.[15] These are large cities and entities and although the ransom amounts they paid may not represent the expenses a San Mateo County public organization could incur, they provide examples of the severity of the potential threat and the enormous costs.

Specifically, the costs of a Ransomware attack could include some or all of the following:[16]

- Direct Costs:
    - Paying the ransom to obtain an encryption key and hoping that it works;
    - Expenditures for outside IT professionals and new systems providers to plan and implement improved breach security based on new Ransomware strategies;

---

[8] National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*. Forward by Clarence Anthony, CEO and Executive Director.

[9] https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-Cybersecurity-insights

[10] Sheehan, Patrick, Ohio Emergency Management Agency, *Cascading Effects of Cyber Security on Ohio*, September 19, 2012

[11] Grand Jury survey responses

[12] MIT Technology Review, *Ransomware may have cost the US more than $7.5 billion in 2019*, January 2, 2020

[13] The Atlanta Journal- Constitution, Stephen Deere. *Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million*. August 2018.

[14] Baltimore Sun, Ian Duncan, Baltimore *estimated cost of ransomware attack at $18.2 million as government begins to restore email accounts*. May 29, 2019.

[15] San Jose Mercury News, David Wu, "*UCSF pays $1.14 million ransom to recover data*", July 4, 2020

[16] https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

  - Paying for enrollments in credit reporting bureaus to stop or correct identity thefts (from the release of previously confidential or secure personal information) for client/customers.
  - Replacing hardware and/or software.
- Indirect Costs:
  - Operations efforts to restore systems and data;
  - Organizational downtime as well as employee overtime;
  - Reputation loss including negative public relations and loss of confidence by the organizations' constituents;
  - Liabilities for legal costs, including defense of lawsuits for breach of private and confidential information and poor handling of personal data.

According to the Coveware Report,[17] the median ransom payment in the first quarter of 2020 was $44,021. This was an increase of roughly 10% over the last quarter of 2019. Public sector entities represented 12% of attacks, about half of which were school systems. The average days of downtime was 15 representing an alarming number of days of inability to service constituents.[18] This underlines an urgent need to understand and evaluate current local governments' Cybersecurity strategies.

The discussion that follows is intended to encourage local public agencies and their IT staff to confidentially evaluate their respective Cybersecurity plans, software and prevention strategies. Since data and systems security are essential to the operation of every public entity in the County, the discussion will not present a specific road map for potential Ransomware-prevention actions but rather establish a "best practice model" that will enhance understanding of the elements essential for an adequate protection plan.

DISCUSSION

In December 2019, the Grand Jury developed an online survey that was sent to all 68 public entities in San Mateo County.[19] Responses were received from 37 of the entities (a 54% response rate). Additionally, follow-up interviews were conducted with three local public IT Managers, one of whom had refused to complete the online survey for fear of disclosing confidential information that could lead to a successful malware or Ransomware attack. These interviewees were questioned regarding the adequacy of Cybersecurity planning and execution. Following a general analysis of local government practices, this report concludes with a review of Cybersecurity best practices which local agencies should consider adopting.

Two Ransomware Attacks Derailed: Best Practices in Action

In order to better understand how to successfully defeat a Ransomware attack, the Grand Jury interviewed an IT Manager of a private enterprise that was attacked twice by Ransomware and was able to fully restore the environment and re-establish workflow within just a few hours.

---

17 https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

18 https://www.msspalert.com/Cybersecurity-research/average-ransomware-payment-rises-again-research/

19 Appendix F

Given the usual secrecy involved in most malware incursions, the following description of this IT manager's actual experience is instructive since it offers an example of "best practices" that can guide others anticipating or facing a Ransomware threat.[20]

This organization suffered two serious breaches less than two months apart and successfully recovered both times. In the first breach, within 45 minutes of a user clicking on an email attachment, the Crypto virus had spread to 12 of the organization's 23 servers. The IT Manager was alerted to the problem both by the user whose PC was locked with the Ransomware demand on his screen and an auto alert from the network scanning software that reported unusual activity.

The IT Manager's first action was to rapidly shut down the entire server network. This of course stopped the spread of the virus, but also prevented users from performing their jobs. Fortunately, their backup strategy implementation worked well as they were able to fully recover within hours.

The major components of the protection strategy employed included:

- Separating the network into discrete departments or segments (creating subnets) which restricted individuals' access to only servers containing their department's software and network storage. This limited the spreading of the virus across various departments within the organization. The analogy is a modern ship with rooms and decks that can be completely closed off from each other in the event of a fire or explosion.
- Taking snapshots (copies) of their Storage Area Network (SAN) twice a day.
- Completing full nightly backups of their SQL databases and incremental backups of the databases at five-minute intervals.
- Performing server backups with a commercial external backup appliance and/or service. See Appendix D for examples of companies in this market.[21]
- Regularly testing the restore process to ensure the successful recovery of critical server hardware. Without testing, there is no assurance that the Cybersecurity plan will work. Moreover, even if it works once, that is no assurance it will work again, without periodic re-testing.
- Conducting weekly backups of critical personnel's full PC hard drives.
- Use the "3-2-1 strategy"[22]: do three backups into two different media including one offsite.

Having all of these Cybersecurity plan components was a good start but it took much more to affect a recovery. First a commercial Virus Removal Software Tool was used which did not work (in this case). Therefore, the IT team used the snapshot copies to replace corrupted data on infected server units followed by the application of the incremental backups of the database to complete the restore.

---

[20] Grand Jury Interview

[21] These services include onsite and offsite backup and recovery services which are usually located outside the immediate locale.

[22] Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy,* January 7, 2020.

This detailed example represents a well thought out and highly prepared plan, executed with precision. The first breach resulted in 4½ hours of downtime as 12 servers were infected. The second breach resulted in 6 ½ hours of downtime to recover 19 affected servers. The IT team was able to recover the servers and their data both times, become fully operational within hours, and the organization did not pay any ransom demands.

Grand Jury Cybersecurity Survey and Follow-up Interviews

Survey question:[23] "*Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?*"

Nine survey responders and one non-survey responder interviewee, a total of 10 of 38 (37 responders to the online survey and one non-survey responder) affirmed an attack had occurred or had possibly occurred in their organization, a 26% "hit" rate. The circumstances of their attacks were reviewed.[24] The non-survey interviewee was the IT manager from a public entity in the County who was unwilling to complete the survey because they did not want to reveal that their organization had been subject to "one or more" Ransomware attacks. Nor were they willing to disclose how successful the Ransomware attack(s) were for fear that they would open themselves up to more attacks.

Survey Question:[25]

"*Is your Information Systems Budget adequate to secure your network properly from malicious attack?*"

Thirty-two of the 37 survey respondents, or 86%, answered Yes to this question. This high percentage of "Yes" responses either indicates a high level of confidence in their defense setup, a reluctance to complain about their IT budget, or as two of our follow-up interviewees revealed[26], a lack of understanding of the complexity of a well-written, well-executed Cybersecurity Plan.[27] Suggesting the latter, The National League of Cities conducted a similar survey of 165 city governments nationwide and asked the same question, ("*Is your budget adequate enough to secure your network properly?*"): 67% replied "No".[28]

Investigation Results Regarding Backup/Restore/Maintenance

The Grand Jury survey and follow-up interviews revealed that, while many local agencies have backup plans,[29] only a portion of those same agencies had successfully recovered lost files from backups and none of the survey responders had ever done a full restore of a server.[30] When an

---

23 Appendix A – Question #1

24 Grand Jury Interview

25 Appendix A – Question #2

26 Grand Jury Interviews

27 Federal Communications Commission, *Cyber Security Planning Guide*, October 2012.

28 National League of Cities report, *Protecting Our Data: What Cities Should Know About Cybersecurity*, page 8

29 Appendix A – Question #3

30 Appendix A – Question #4

attack occurs with inadequate backup processes in place, there is no way to recover. Moreover, a proactive and well-thought-out business continuity plan is something that all system and data administrators must embrace.

What is a good backup strategy? Certain applications provide the ability within the applications themselves to set up different types of backups and schedule them to be performed automatically. A good example of this is SQL.[31] Using a SQL-based approach, both nightly full database backups can be scheduled as well as intermittent transaction log backups (which capture activity during small time increments), so that a recovery could be completed with virtually no loss of data. These backups should then be stored according to the 3-2-1 backup rule[32] whereby three copies or versions are taken, stored on two different media, one of which is offsite. Operating systems and third-party vendors offer a multitude of backup solutions for servers. Snapshots or image backups[33] provide the most complete backup and the fastest restore option.[34]

Raj Samani, Chief Technology Officer for Europe at Intel Security captures the importance of a complete backup strategy, "Most Ransomware attacks can be avoided through good cyber hygiene and effective, regular data backups that are continually tested to ensure they can be restored if needed."[35]

As this discussion shows, the technology to prevent and if necessary, correct, the impact of a malware attack is available. Local government agencies must be pro-active and vigilant in using such to protect their data and their businesses.

Investigation Results Regarding Employee Training

Education is the best defense. "Preventing infection is far easier than correcting the situation as most of the infections are acquired either from a socially engineered email (one that appears reputable or from a familiar source), or from visiting an infected website, so controlling risk on your side is the easiest method."[36]

Answers to Survey Question #5 provide strong evidence for the need for the governing boards to review with their IT managers their defenses against cyberthreats: "*Do you provide training to employees regarding malware?*" 12 responded with a non-qualified "Yes". Nine responded "No" (24%) and 16 responded with a qualified "Yes" (42%) and described their training as needing improvements.[37] As one survey responder commented, "The answer is yes, but a lot more needs to be done."

---

31 Structured Query Language (SQL) is a programming language

32 Management Wire, *The 3-2-1 Backup Rule and Effective Cybersecurity Strategy,* January 7, 2020.

33 Image backup consists of block by block storing of the contents of a hard drive

34 https:\\www.ltnow.com/file-backup-vs-image-backup-which-is-best/

35 Zerto, Raj Samani, *Ransomware – Mitigating the Threat of Cyber Attacks, 2019*

36 Epicor, *Protecting Yourself from Ransomware,* January 2020

37 Grand Jury Survey responses

Cybersecurity training is a well-established industry – providing a focused set of classes and materials designed to reduce users' clicks on harmful links and attachments. Security training, awareness, and assessment should be a routine part of the Cybersecurity strategy in government. Deploying such a program covers the education, training and testing of employees to recognize, delete and report attempted attacks. Studies show these programs reduce but do not eliminate user error.

Government Technology magazine captured it best in their cover story entitled "In the quest to guard against cyberthreats, can we solve the people problem? The Weakest Link."[38] The article concluded that even with the best training programs and defenses, the human element may never be completely overcome.[39] This is precisely why recurring training and user testing is encouraged by best practices.

Handling Incoming Emails – Phishing Defenses

In a worldwide survey of Managed IT Service Providers (MSP's) in 2019, "67% of Ransomware attacks originated from a phishing or spam email…the easiest method of delivery and man does it pay off."[40] The greatest threats take advantage of users "within" the network, i.e., users who click on malicious links or open email attachments that contain viruses or make other mistakes that allow hackers to gain access to the entity's system or network. Trend Micro estimates that the vast majority of all attacks occur when a user clicks on something they should not.[41]

There are different ways to help the user community recognize and protect against a phishing attack. Most network environments utilize spam filters to automatically filter incoming messages. Spam filters are used to detect unsolicited, unwanted, and virus-infested email and stop it from getting into email inboxes.[42] "Additionally, malware detection software can also be highly successful in reducing the risk of Ransomware but the anti-malware definitions (a database of known infectious code) need to be constantly updated…which takes effort and time but represents the single most effective defensive strategy."[43]

Message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content. An administrator can set up message rules on a users' client or the email server. An example of a message rule might be if the sending organization includes *@smithco.com* in the sender's address, the message is automatically moved the incoming message into a personal folder called "Smith Company." A better example would be a rule that flags all external emails (not from the host's domain) and warns about the threats of clicking on attachments or weblinks. An example of this visual potential threat message rule is displayed in Appendix C.

---

38 Government Technology Magazine, Adam Stone, *The Weakest Link*, Oct/Nov 2018

39 Ibid

40 VadeSecure – Predictive Email Defense, *Ransomware Attacks: Why Email is still the #1 Delivery Method"*, January 16, 2020

41 https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

42 https://www.mailchannels.com/what-is-spam-filtering/

43 Epicor, *Protecting Yourself from Ransomware"*, January 2020

Message rules can be very powerful to alert users of potential threats or to be careful about what they might click on and endanger their system. Some of the vendors listed in Appendix B also can "report" a suspected phishing attempt to an IT administrator. The Grand Jury's review revealed that some of the Information Technology Services departments for local public entities have installed message rules on their email servers to notify users of external emails.[44] This is a "best practice" which all local governmental agencies should consider.

Phishing emails are easy to create, as they do not take a high level of skill to provide the illusion of legitimacy by mimicking web-site brands or using logos from Google images. They can also easily spoof (fake) an email address to look like a trusted source.[45] It can often be very difficult to catch these risky emails, as the spoofed emails are cleverly disguised. A YouTube video created by Cisco Systems illustrates the sophisticated approach a phishing email may take – "Anatomy of an Attack".[46] It shows an attacker constructing a realistic identity deception email and can be viewed at https://www.youtube.com/watch?v=4gR562GW7TI After you watch this video please note, had an email filter caught this message and flagged it as external and warned about clicking on links, the deception may have been caught.

What Does Excellent Cyber Defense Look Like?

Survey Question[47]: *"What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)"*

Five survey responders did not divulge the infrastructure of their environment. 17 responders provided abbreviated details indicating they do have Cybersecurity protections in place. The remaining 15 responses were explicit about their organizations' hardware and software defense strategies. Below is a survey response that illustrates a well-protected environment using some of the best practices of Cybersecurity:

"At the first layer, we use a PAN 220 Firewall with all subscriptions enabled, (URL Filtering, Antivirus/Vulnerability, Wildfire, etc.), block all international countries both in and outbound. Once traffic is passed for email, it passes through a Barracuda spam filter, filtering and scanning phishing and virus emails, checks with External Reputation servers for known virus and spamming servers, then passes to an on-premise exchange server. The exchange servers have another layer installed, Symantec Antivirus, giving a third layer of scanning. All servers and workstations have the latest version of the antivirus installed controlled by a centralized server. Window patches are applied on a monthly basis to all servers and workstations, and servers are retired once Microsoft ends support for an operating system." [48]

The survey respondent's best practices:

- Filtering incoming email for viruses, malware, and phishing attempts;
- Utilizing protection software from multiple vendors;
- Utilizing multiple layers of defense;

---

44 Grand Jury interviews

45 Ibid

46 Cisco Systems, *Ransomware - Anatomy of an Attack,* https://www.youtube.com/watch?v=4gR562GW7TI

47 Appendix A - Question #6

48 Grand Jury Survey response

- Keeping systems up-to date.

Breaches and attacks that manage to extract data (Ransomware 2.0) expose additional risks to sensitive information. Security professionals point out additional options for securing organizational data:[49]

- Use Subnets[50] to section out servers with separate security permissions and limited access;
- Disable and block unused services, protocols and ports;
- Perform Backup & Recovery (focus on full testing of recovery);
- Strengthen the password policy (long, complex, with expiration dates);
- Employ 2-factor authentication (password then keycode) for external user access.[51]
- Install Anti-malware / Antivirus software on all machines and keep current (update at least monthly);
- Update at least monthly, patches for operating systems, firewalls, spam filters, malware, and other key applications;
- Perform monitoring and auditing of failed logins, password changes, resource usage, and services stopping.

Local public entities can get assistance from The Federal Communications Commission's (FCC) Cyber Security Planning Guide that includes a customized Cyber Security Planning Tool to craft and execute a customizable Cybersecurity plan.[52] As their introduction explains, "data security is crucial … customer and client information, payment information, personal files, bank account details … all of this information is often impossible to replace if lost and dangerous in the hands of criminals… losing (your data) to hackers or malware infection can have far graver consequences."[53] Public entities should take advantage of this Guide in reviewing the current status of their own data system security.

When answering questions of respondents via email it was found that some already use cloud hosting for email.[54] During the interviews it was further uncovered that a school IT manager is considering additional cloud hosting of one or more of their applications. Cloud providers are able to provide layers of protection for a customer's network and software, as well as creating a segregation between their network and their customers. A cloud provider will patch and maintain current software versions, leverage security and malware and have a dedicated security team (24x7x365) that is responsible for staying on top of the security risks.[55]

---

49 Government Technology Magazine, Adam Stone, *The Weakest Link,* Oct/Nov 2018

50 https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

51 The County's Office of the Assessor-County Clerk-Recorder and Elections has already instituted 2-factor authentication. 2018-2019 Grand Jury Report – Security of Election Announcements.

52 Federal Communications Commission, *Cyber Security Planning Guide* https://transition.fcc.gov/cyber/cyberplanner.pdf and FCC *Cyber Security Planner* (customizable) https://www.fcc.gov/cyberplanner

53 Ibid, page PDS-1

54 eMails received from public domain accounts

55 Government Technology Magazine, Adam Stone, *The Weakest Link,* Oct/Nov 2018

Conclusions

Grand Jury survey results and in-depth interviews determined that some local government agencies have Cybersecurity strategies in place. For them, this report is asking those IT departments to re-challenge the sufficiency of their employee training, the regular (full) testing of their defense strategies and the adequacy/age of their Cybersecurity strategy including consideration of cloud hosting. For the rest, this is a good time to complete a review and see what additional measures can be taken to beef up their IT security using the information provided in this report as a guide. The biggest trap is believing that a malware attack, or in the worst case a Ransomware attack, is unlikely to happen to organizations and that the Cybersecurity strategies already in place are sufficient to successfully recover.

As learned from the best practices example of the IT manager who thwarted two attacks successfully, a comprehensive Cybersecurity plan includes user prevention steps, spam and malware software, back-ups and full recovery testing. These suggestions as well as those from the professional literature on Cybersecurity include the following list of best practices:

- Anti-Malware definitions need to be constantly updated to retain their effectiveness.
- Software updates need to be kept current.
- To identify external emails, message rules can be used to flag external emails and thereby decrease the probability that a user clicks on bad content.
- To thwart phishing attempts, footers can be added to incoming emails to warn about opening attachments and clicking on links (see Appendix C).
- Security training, awareness and assessment need to be routine along with testing all employees to recognize, delete and report attempted attacks (See Appendix B).
- Establishing a thorough and comprehensive backup process for all Servers using the 3-2-1 rule and establishing a separate backup process for key users' critical folders (e.g., administration, accounting, human resources) to be able to restore/recover from a secure onsite and/or offsite backup.
- Snapshots and/or image backups provide the most complete backup and the fastest recovery option.
- Consider cloud-hosting of email and other applications to provide added security, backup & restore capabilities and filtering benefits to close the largest and easiest route for Ransomware to penetrate entity systems.

FINDINGS

F1. Ransomware is a real and growing threat to public entities including those in San Mateo County.

F2. Across the country, local governments and schools represent 12% of all Ransomware attacks.

F3. The direct and indirect costs of Ransomware can be significant.

F4. Cybersecurity reviews and assessments, and an updated, well-executed Cybersecurity plan, are critical components of IT security strategy.

F5. A comprehensive Cybersecurity plan should include, at a minimum, information concerning prevention steps, spam and malware software, and backups and full recovery testing.

F6. The identification of phishing attempts, including the use of spam filters, is an important component to protecting an IT system from Ransomware attacks.

F7. Testing a full restore of a server to ensure that backups are reliable should be undertaken regularly as part an entity's backup plan to recover lost information.

F8. Training of new employees, and the recurring training of existing employees, is an important component of defense against Ransomware.

RECOMMENDATIONS

The Grand Jury recommends that each governing body undertake its own confidential effort to protect against Ransomware attacks. Specifically:

R1. Each of the governmental entities in San Mateo County with an IT department or IT function (whether in-house, handled by another government unit or outsourced to a private enterprise) as listed in Appendix F, should by November 30, 2020, make a request for a report from their IT organization that addresses the concerns identified in the report, specifically:

1. System Security (Firewalls, Anti-malware/Antivirus software, use of subnets, strong password policies, updating/patching regularly)
2. Backup & Recovery (In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a Server from a backup?)
3. Prevention (turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content)

R2. These confidential internal reports should be provided to the governing body by June 30, 2021. This report should describe what actions have already been taken and which will be given timely consideration for future enhancements to the existing cybersecurity plan.

R3. Given the results of their internal reports, governmental entities may choose to request further guidance by means of a Cybersecurity review from the U.S. Department of Homeland Security[56] and/or a cyber hygiene assessment from the County Controller's Office.[57]

---

[56] https://www.us-cert.gov/resources/assessments

[57] 2018-2019 San Mateo Grand Jury Report – Security of Election Announcements

R4. Given the results of their internal reports, governmental entities may choose to ask their IT departments to review their own Cybersecurity Plan with the detailed template provided by the FCC's Cybersecurity Planning Guide and consider customizing it using FCC's Create Custom Cybersecurity Planning Guide tool (see footnote 52).

METHODOLOGY

Documents

- Attack incident reports were requested from IT Departments who experienced attack(s). No incident reports were received.

Site Tours

- No site tours were performed as a part of this report.

Interviews

Reports issued by the Civil Grand Jury do not identify individuals interviewed. Penal Code Section 929 requires that reports of the Grand Jury not contain the name of any person or facts leading to the identity of any person who provides information to the Civil Grand Jury.

- Three Information Systems Managers of three different public entity IT organizations.
- Two non-public professional IT Managers. Both of these Managers' IT infrastructure environments had been infected with Ransomware attacks. One paid the ransom and the other did not.
- A professional Ransomware expert who often consults with companies who have been attacked or desire assistance preventing attacks. He also teaches classes on preparing for and preventing Ransomware attacks.
- Numerous security industry professionals at the RSA Conference held at Moscone Center in San Francisco between February 24th and 28th 2020.

BIBLIOGRAPHY

Anslinger, Joe. *"File Backup vs. Image Backup – Which is Best?"* Lieberman Technology. June 11, 2013. https://www.ltnow.com/file-backup-vs-image-backup-which-is-best/

Cisco Systems. *Ransomware - Anatomy of an Attack.* https://www.youtube.com/watch?v=4gR562GW7TI

Coveware, *"Ransomware Payments Increase In Evolving Distribution of Enterprise Ransomware Variants."* April 29, 2020. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

Davis, Jessica. *"As Ransomware Attacks Increase, DHS Alerts to Cybersecurity Insights."* Health IT Security, September 9, 2019. https://healthitsecurity.com/news/as-ransomware-attacks-increase-dhs-alerts-to-cybersecurity-insights

Deere, Stephen. *"Confidential Report: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million."* The Atlanta Journal- Constitution. August 2018.

Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA). *"Assessments: Cyber Resilience Review (CRR)"* https://www.us-cert.gov/resources/assessments

Duncan, Ian. *"Baltimore Estimated Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts."* Baltimore Sun, May 29, 2019.

Epicor Corporation. *Protecting Yourself From Ransomware*. January 2020.

Fadilpasic, Sead. *"Welcome to the era of Ransomware 2.0"* ITProPortal. February 12, 2020. https://www.itproportal.com/news/welcome-to-the-era-of-ransomware-20/

Federal Communications Commission. *Cyber Security Planning Guide.* https://www.fcc.gov/cyber/cyberplanner.pdf

Gutman, Yotam. *"What is the True Cost of a Ransomware Attack."* SentinelOne. January 8, 2020. https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

Iloh, Raphael. *"The 3-2-1 Backup Rule and Effective Cybersecurity Strategy."* Management Wire. January 7, 2020. https://www.managementwire.com/the-3-2-1-backup-rule-and-effective-cybersecurity-strategy/

Jendre, Adrien." *Ransomware Attacks: Why Email Is Still the #1 Delivery Method."* Vade Security. January 16, 2020. https://www.vadesecure.com/en/ransomware-attacks-why-email-is-still-the-1-delivery-method/

Kass, DH. *"Average Ransomware Payment Rises Again: Research."* MSSP Alert. April 30, 2020. https://www.msspalert.com/cybersecurity-research/average-ransomware-payment-rises-again-research/

Kraft Technology Group. *"When Was The Last Time You Tested Your Business Backups?"* https://www.kraftgrp.com/when-was-the-last-time-you-tested-your-business-backups/

MailChannels. *"What is Spam Filtering?"* https://www.mailchannels.com/what-is-spam-filtering/

MIT Technology Review, *"Ransomware May Have Cost the US More Than $7.5Billion in 2019."* January 2, 2020. https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/

National League of Cities Report. *"Protecting Our Data: What Cities Should Know About Cybersecurity."* Forward by Clarence Anthony, CEO and Executive Director.

Pearson Education. *Ubuntu Unleashed.* 2015 Edition. Page 655.

Ranger, Steve. *"What is cloud computing? Everything you need to know about the cloud explained."* ZD Net, December 13, 2018. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/

Samani, Raj. *"Ransomware – Mitigating the Threat of Cyber Security Attacks."* Zerto. 2019. https://www.zerto.com/wp-content/uploads/2019/09/ransomware-mitigating-the-threat-of-cyber-security-attacks.pdf

San Mateo Grand Jury Report. *Security of Election Announcements*. 2018-2019.

Search Networking, *"Protocols, Lesson 6: IP subnetting - The basic concepts."* October 2004. https://searchnetworking.techtarget.com/tutorial/Protocols-Lesson-6-IP-subnetting-The-basic-concepts

Sheehan, Patrick. *"Cascading Effects of Cyber Security on Ohio."* Ohio Emergency Management Agency. September 19, 2012.

Stone, Adam. *The Weakest Link.* Government Technology Magazine, October/November 2018.

Trend Micro. *"Online Phishing: How To Stay Out Of The Hackers' Nets"* November 20, 2019. https://blog.trendmicro.com/online-phishing-how-to-stay-out-of-the-hackers-nets/

Wu, David. *"UCSF pays $1.14 Million Ransom to Recover Data."* San Jose Mercury News. July 4, 2020.

APPENDIX A – SURVEY QUESTIONS

1. Has your Organization had a Ransomware attack? Specifically, has there been an instance or multiple instances when an attack has locked up a computer or computers and presented a demand for ransom to unlock the infection?

If you answered Yes or Possibly to Question 1, please provide a detailed description of the attack. What actions were taken once the attack was realized?

2. Is your Information Systems Budget adequate to secure your network properly from malicious attack?

3. Please provide an explanation of your Systems Backup processes? How often are backups run, where do you store the Backups?

4. Have you ever had to Restore from Backups? Please describe in detail why you did the Restore and describe the process used.

5. Do you provide training to employees regarding Malware?

6. What defenses do you currently employ to block malware? Please be specific. (Firewall brand/model, Software filters/spam blocker, etc.)

APPENDIX B – EMPLOYEE TRAINING OPTIONS

Phishing is the primary method of entry in cyber-attacks worldwide. Over the past few years, some security industry companies have come up with excellent testing, training, monitoring, measuring and reporting solution to help with employee training. The primary goal of an employee training program is to change user's behavior when viewing emails that might contain threats.

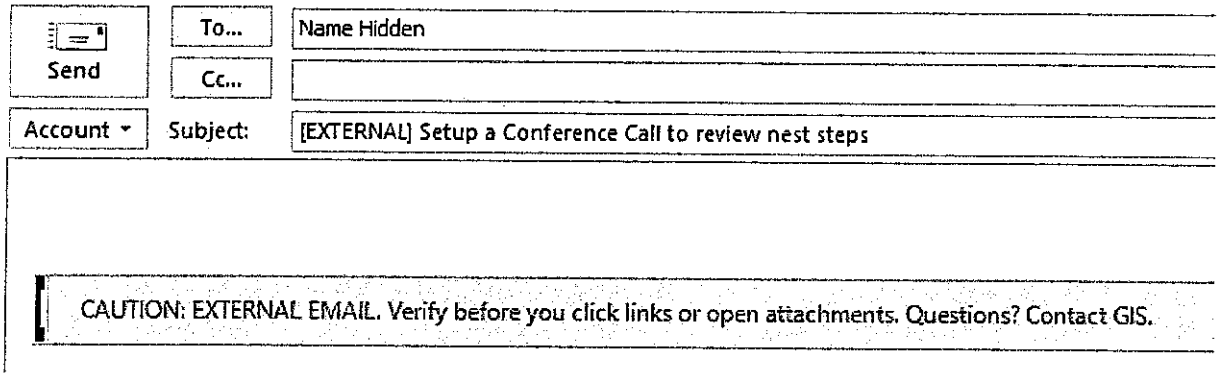
The typical components of these solutions include:

- Customized phishing attacks designed to test employees in spotting attack attempts
- Provide users a simple to use reporting tool to flag suspected attacks
- An incidence response platform for controlling the spread of an attack
- Reporting dashboards tracking user click-throughs
- Employee training programs

Here are some website links for the companies offering training solutions.
www.knowbe4.com
www.lucysecurity.com
www.metacompliance.com
www.mediapro.com
www.cofense.com
www.elevatesecurity.com
www.securitymentor.com

www.habitu8.io

APPENDIX C – EMAIL MESSAGE RULE - EXTERNAL



APPENDIX D – BACKUP & RECOVERY APPLIANCES & SERVICES

There are a large number of companies that provide Backup and Recovery solutions. Solutions Review has prepared a buyer's guide for the leading vendors. Click on the following link or copy and paste this URL into a browser to get your own copy of this guide.

https://solutionsreview.com/backup-disaster-recovery/get-a-free-backup-and-disaster-recovery-buyers-guide/

Specifically, some of the vendors in this report do not provide appliances, only virtual server support. Here is a partial list of appliance and solution vendors:

www.unitrends.com
www.barracuda.com
www.carbonite.com
www.commvault.com
www.dellemc.com
www.axcient.com
www.cohesity.com
www.datto.com
www.infrascale.com

APPENDIX E – PHISHING DEFENSE VENDORS

Some companies that provide solutions that improve email defenses are:

https://www.opswat.com/products/metadefender/email-gateway-security
https://www.agari.com/products/phishing-defense/
https://www.inky.com/anti-phishing-software
https://www.mimecast.com/products/email-security-with-targeted-threat-protection/

APPENDIX F: PUBLIC ENTITIES IN SAN MATEO COUNTY (68)

City/Town Governments (20)
- Town of Atherton
- City of Belmont
- City of Brisbane
- City of Burlingame
- City of Colma
- City of Daly City
- City of East Palo Alto
- City of Foster City
- City of Half Moon Bay
- City of Hillsborough
- City of Menlo Park
- City of Millbrae
- City of Pacifica
- Town of Portola Valley
- City of Redwood City
- City of San Bruno
- City of San Carlos
- City of San Mateo
- City of South San Francisco
- Town of Woodside

County Government (1)
- County of San Mateo, Information Services Department

School Districts (25)
- Bayshore Elementary School District
- Belmont Redwood Shores School District
- Brisbane School District
- Burlingame School District
- Cabrillo Unified School District
- Hillsborough City School District
- Jefferson Elementary School District
- Jefferson Union High School District
- La Honda Pescadero School District
- Las Lomitas Elementary School District
- Menlo Park City School District
- Millbrae School District
- Pacifica School District
- Portola Valley School District
- Ravenswood City School District
- Redwood City School District
- San Bruno Park School District
- San Carlos School District

San Mateo Foster City School District
San Mateo Union High School District
Sequoia Union High School District
San Mateo County Community College School District
San Mateo County Office of Education
South San Francsico Unified School District
Woodside School District

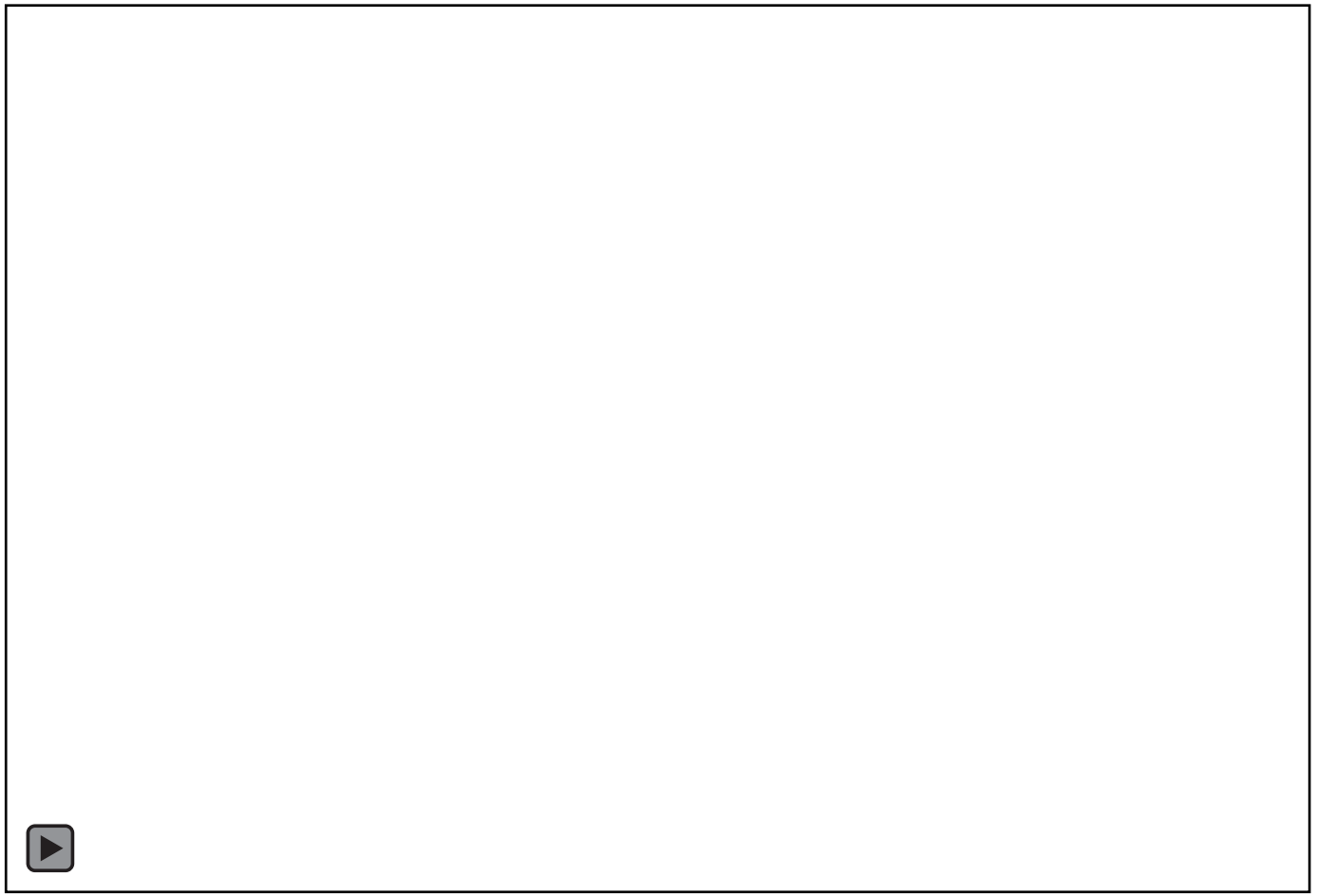
Independent Special Districts (22)
Bayshore Sanitary District
Broadmoor Police Protection District
Coastside County Water District
Coastside Fire Protection District
Colma Fire Protection District
East Palo Alto Sanitary District
Granada Community Services District
Highlands Recreation District
Ladera Recreation District
Menlo Park Fire Protection District
Mid Peninsula Regional Open Space District
Mid-Peninsula Water District
Montara Water and Sanitary District
North Coast County Water District
Peninsula Health Care District
San Mateo County Harbor District
San Mateo County Mosquito and Vector Control District
San Mateo County Resource Conservation District
Sequoia Healthcare
West Bay Sanitary District
Westborough Water District
Woodside Fire Protection District

Not Included: County-governed special districts and subsidiary special districts governed by their respective city councils.

Issued: October 7, 2020

Cyber Security Presentation (Anti-Malware/Phishing)

Jimmy Kimmel Live - What is Your Password?



Topics for Discussion

- Importance of Awareness
- Phishing
- Common Examples
- Spear Phishing
- Recognition
- Prevention
- Ransomware
- Social Engineering
- Other Safety Tips

Importance of Awareness: You are the target…

- You, and your access to City data, are the primary target of hackers.
- Gaining access to your login information allows them to impersonate you, or use your computer, to gain access to city systems and data.
- IT can address only a portion of security risks.
- Most Commonly Compromised
  - End User Access
- Allows Bad Actors to
  - Impersonate End Users
  - Access Files
  - Send/Receive email
  - Steal data/information

Phishing: What is it?

- **Phishing** – Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses
  - Designed to trick you into clicking a link or providing personal or financial information
  - Often in the form of emails and websites
  - May appear to come from legitimate companies, organizations or known individuals
  - Take advantage of natural disasters, epidemics, health scares, political elections or timely events

Types of Phishing

- **Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- **Spear Phishing** – Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect
- **Whaling** – Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access
- **Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source
- **Advance-Fee Scam:** Requests the target to send money or bank account information to the cybercriminal

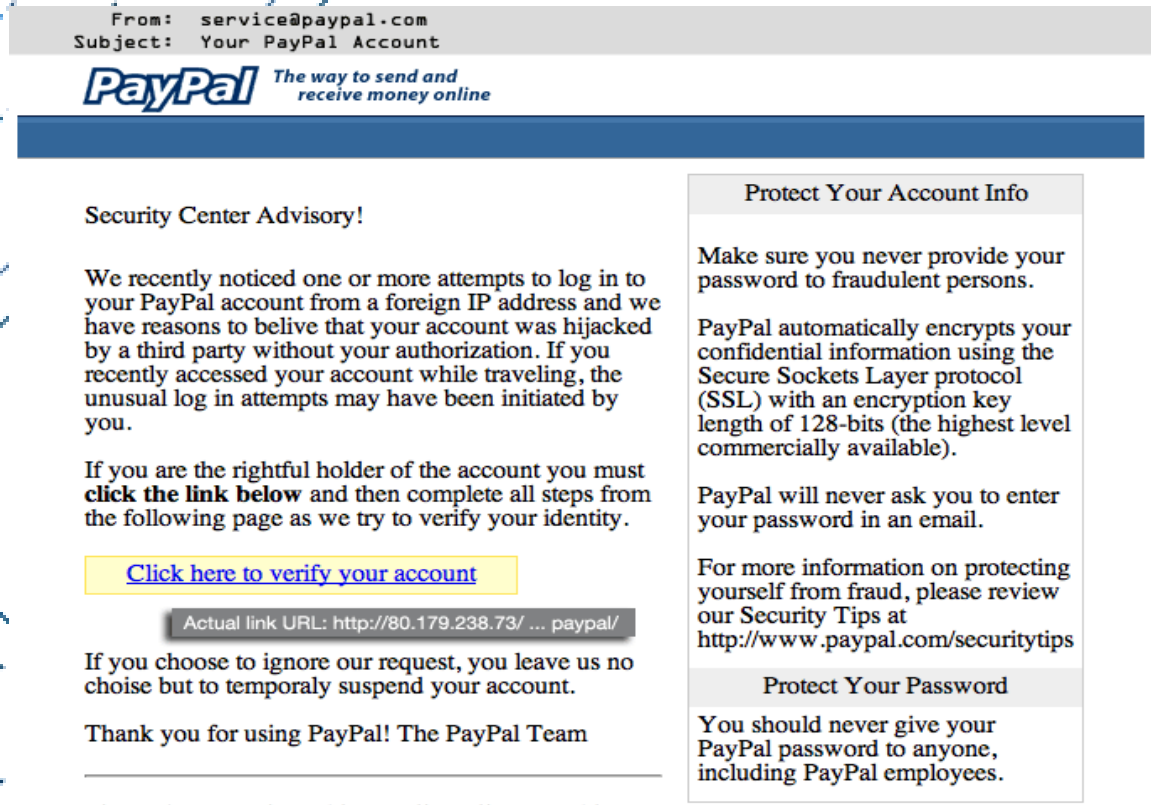
Common Baiting Tactics

- **Notification from a help desk or system administrator**
  Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.
- **Advertisement for immediate weight loss, hair growth or fitness prowess**
  Serves as a ploy to get you to click on a link that will infect your computer or mobile device with malware or viruses.
- **Attachment labeled “invoice” or “shipping order”**
  Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.
- **Notification from what appears to be a credit card company**
  Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.
- **Fake account on a social media site**
  Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

Hidden Threats

- Phishing not only attempts to get sensitive info
- Can include malicious software
- Attachments, Emails, Links, Files
  - May contain programs that
    - May capture your keystrokes
    - Capture your personal files
    - Send data offsite
    - Encrypts data and requests a ransom

Common Examples



From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

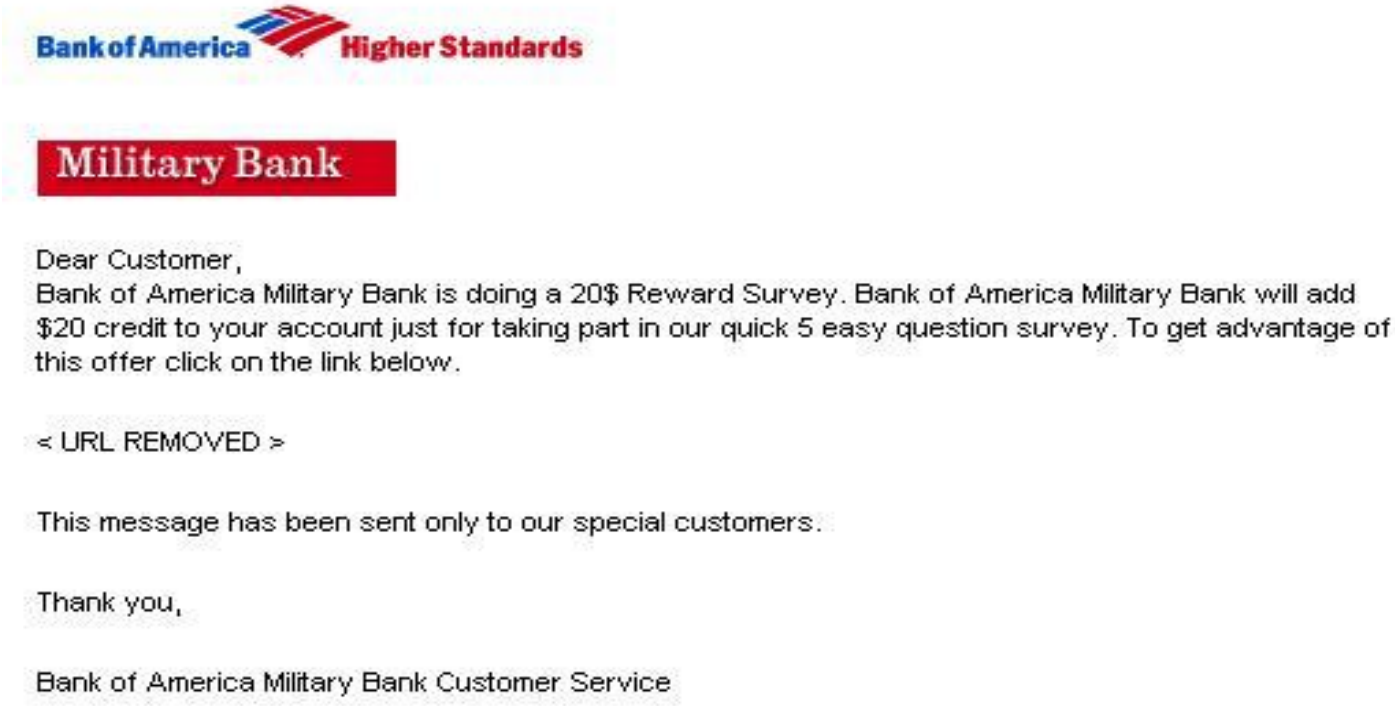
You should never give your PayPal password to anyone, including PayPal employees.

Phishing is not new and many of you have seen examples in emails

- You may have seen emails that appear to come from your bank or other online financial institutions.
- Commonly Seen Commercial Examples:
  - eBay, PayPal, all banking and financial institutions

Common Examples

Phishing Email sent portraying Bank of America,
Entices the user to complete a survey and receive a $20 credit.



Bank of America Higher Standards

Military Bank

Dear Customer,
Bank of America Military Bank is doing a 20$ Reward Survey. Bank of America Military Bank will add $20 credit to your account just for taking part in our quick 5 easy question survey. To get advantage of this offer click on the link below.

< URL REMOVED >

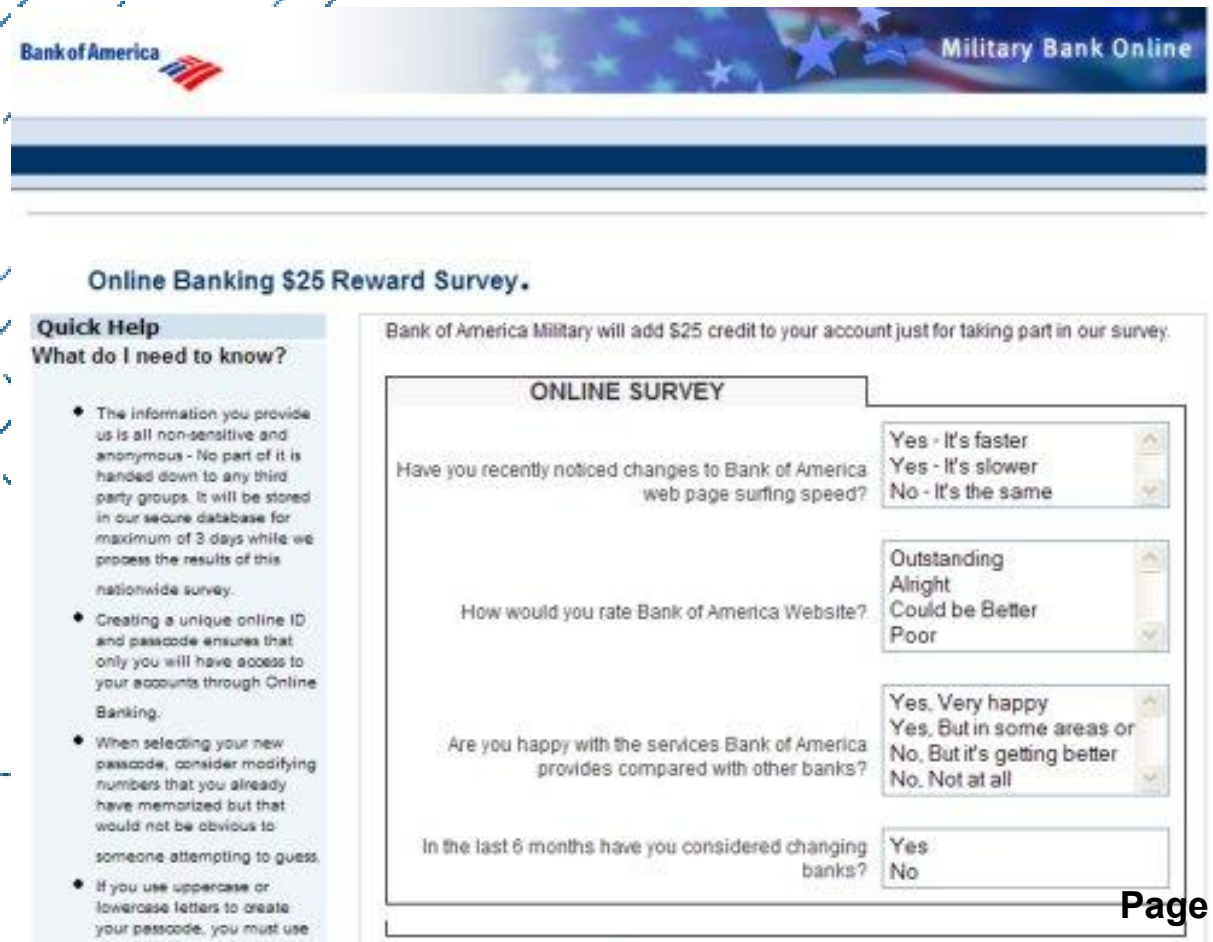
This message has been sent only to our special customers.

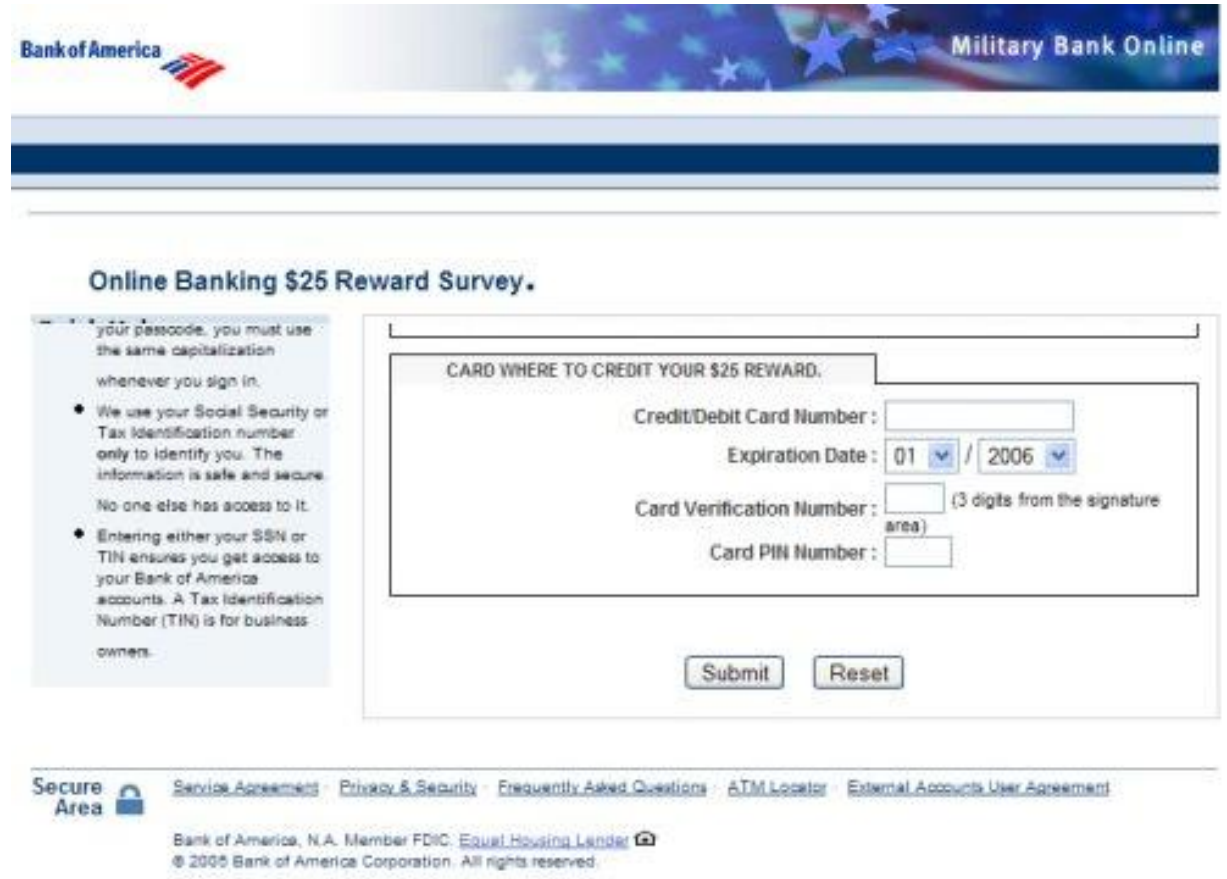
Thank you,

Bank of America Military Bank Customer Service

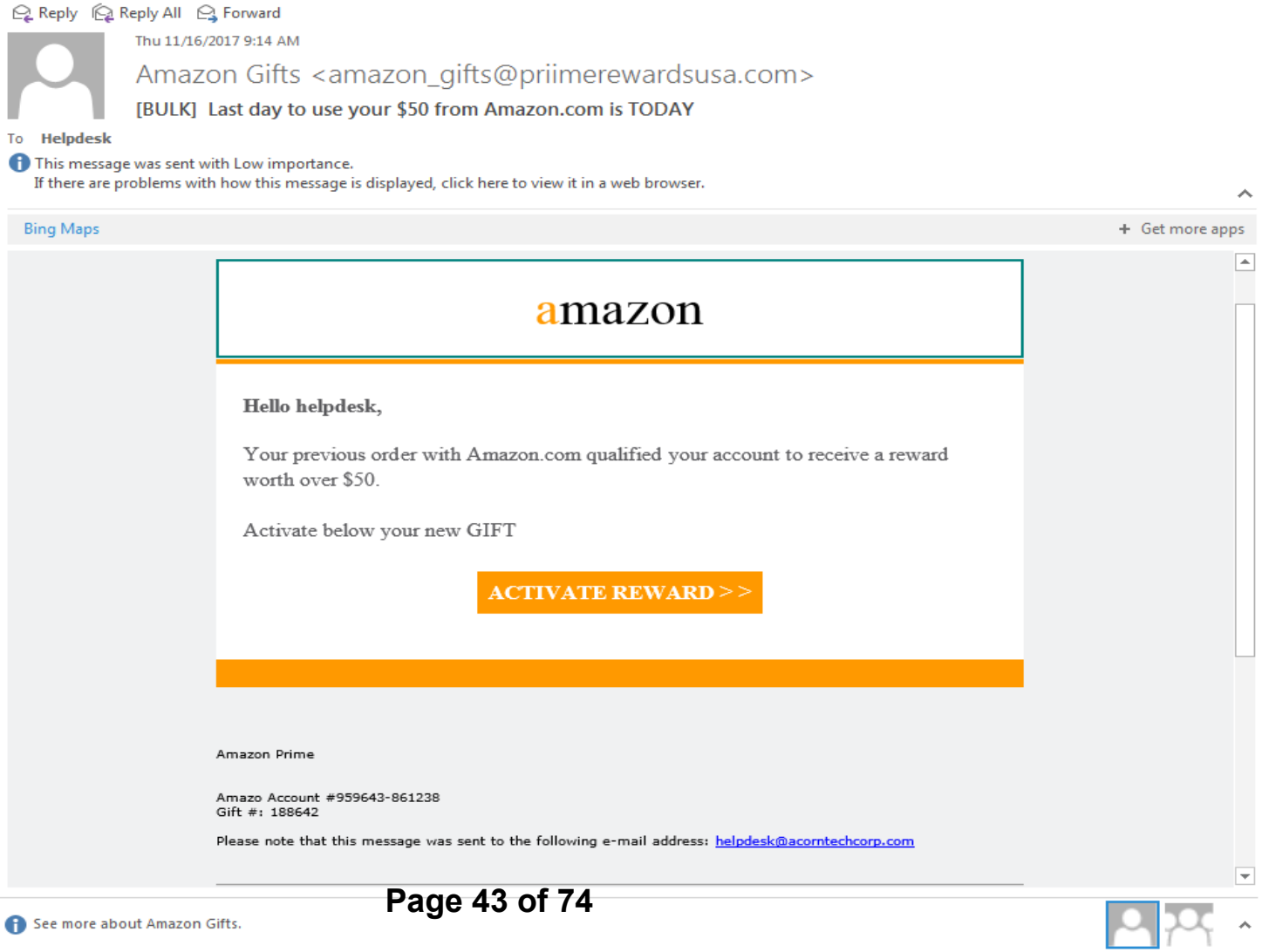
Common Examples

Convincing website linked from BOA email





Common Examples



Common Examples

From: VoiceMail System [mailto:newvoicemai@www.ee.co.uk]
Sent: Monday, November 05, 2018 7:11 AM
To: [redacted]
Subject: (800) 829 4933 left you a voice message

Microsoft Office 365

A voice message was received from **+1 (800) 829 4933** on **November 05, 2018** at **09:58 AM**.

Message ID: **VOM-05-11-2018** | Length: **0:52 secs**

Listen to Voice Message Now

https://www.tinyurl.com/november5voicemail2018
Click or tap to follow link.

You can save this message here: Recorded Voice-Message.wav

Thank you.

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

You are receiving this email because you have subscribed to Microsoft Office 365.
Copyright 2017 Microsoft Corporation Privacy Statement

Spear Phishing

Spear Phishing is an even greater threat

- A highly targeted phishing attempt
- The recipient (target) is selectively chosen
- Usually with an understanding of the target
- With a specific attack attempt

Spear Phishing

The attacker may:

- Address the recipient by name
- Use jargon of the organization
- Reference actual procedures, purchase orders, and invoices

The email may appear very genuine

- “Spoof” the senders email address
- Directly address the recipient
- Relevant subject line content
- Request actions to get info, data, or $$

Spear Phishing Example

Targeted plausible payment request.

DO NOT SEND MONEY BEFORE CONFIRMING WITH SENDER

---------- Forwarded message ----------
From: **Ms. Amy E. Ferrer** <admin345@inbox.lt>
Date: Wed, Jun 7, 2017 at 2:03 PM
Subject: Transfer request
To: [redacted]@udel.edu

Hello, [redacted]

I will need you to process a wire transfer of $14,545.90 which needs to go out today as a same value day payment. We have a pending invoice from our new Vendor, I have asked them to send a copy of invoice hopefully i should received it later today.

Let me know if you are available so i can forward the beneficiary account

Kind regards,

Amy E. Ferrer

sent from my iPad

Should I be worried?

- **Occurs in organizations everyday**
- **Attacker's primary focus is to get you to:**
  - **Open an attachment**
  - **Follow a web link**
  - **Install the malicious software**

- **If you receive an email that is out of the ordinary or unexpected:**
  - **Always confirm with the sender**
  - **Even if you are familiar with them**
  - **Their account may be compromised**

Recognition

Other recognition factors of phishing attempts:

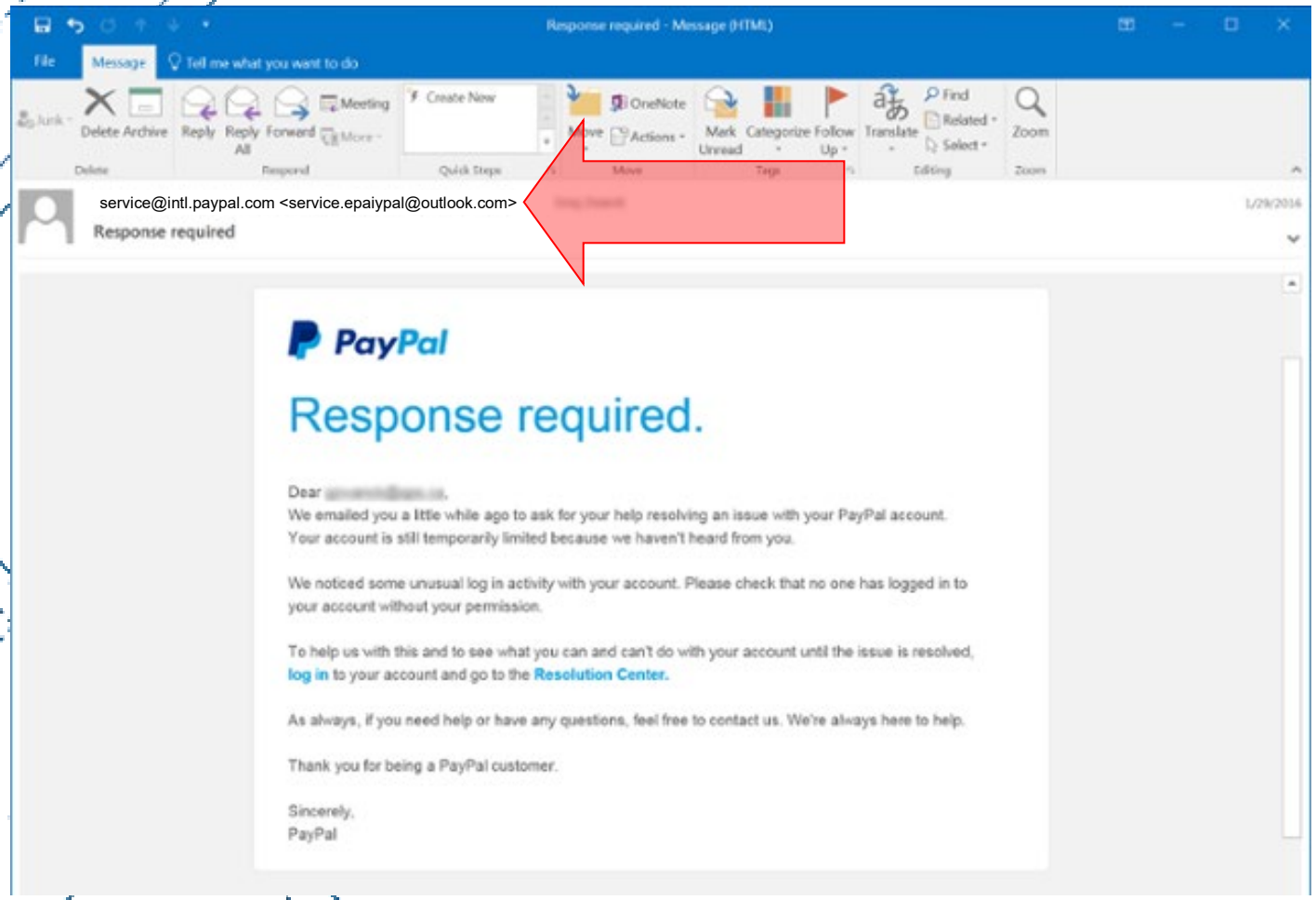
1. Generic Greeting
2. Fake Sender's Address
3. False Sense of Urgency
4. Fake and deceptive web links
5. Requires you follow a link
6. Requires you to "sign up" for a great deal
7. Requires you to log in and verify your account
8. Encourages you to view/read an attachment
9. Emails that appear like a website
10. Misspellings and bad grammar

Recognition

- "From" field of an email can be easily faked (spoofed).
  - It might appear completely correct, or have a similar variation.
  - account_security@mypay.com
- On the other hand, the message may come from a
  - legitimate email account, because that account has been compromised.
  - john.smith.yourboss@yourbusiness.com

This can occur when the attackers obtain someone's login credentials and email contacts in their address book in order to obtain more accounts.

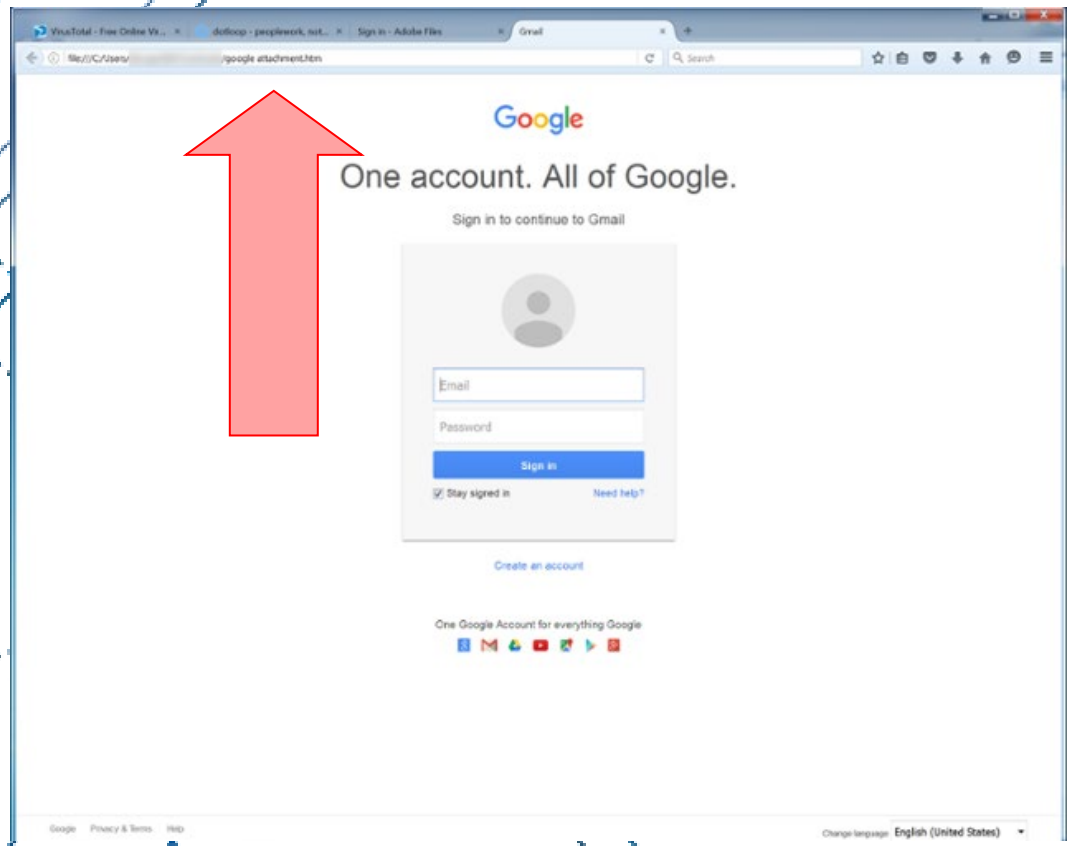
Recognition (Example 1)

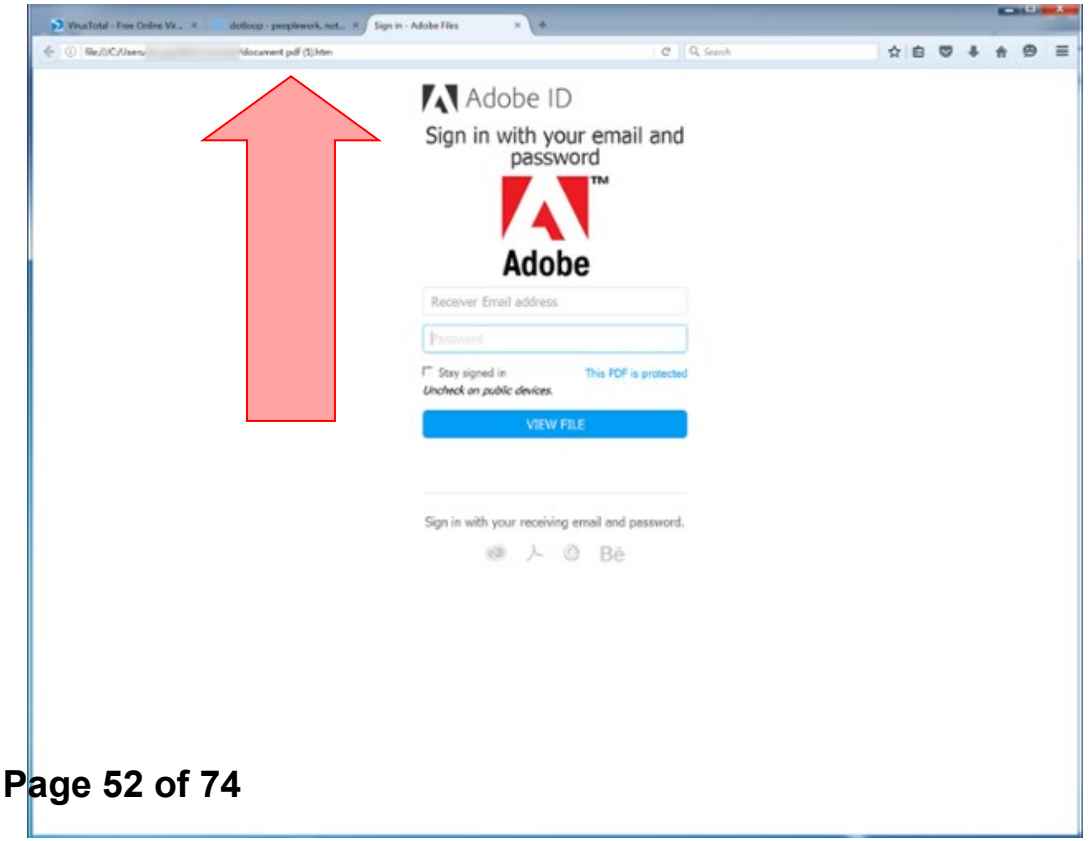


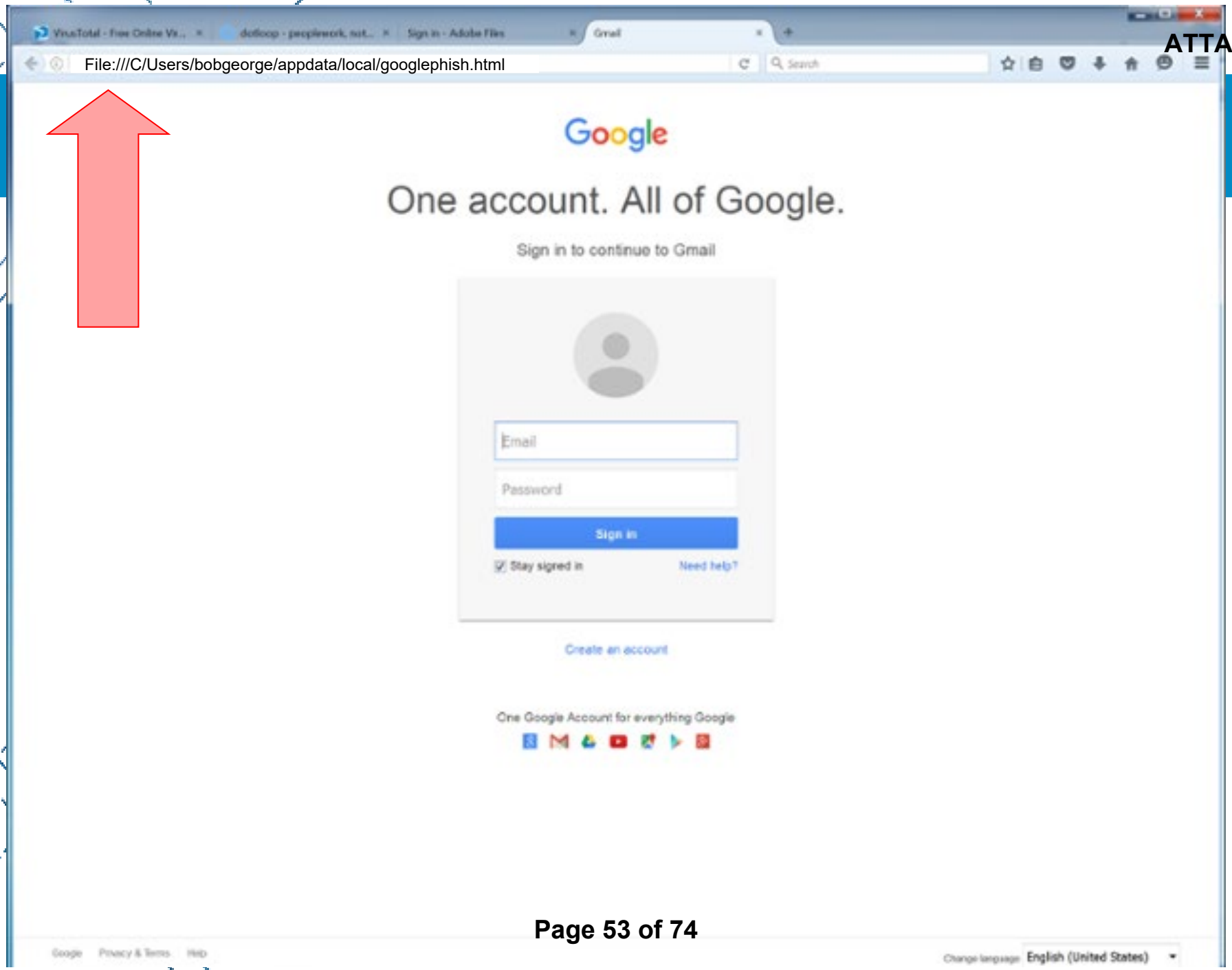
Example of a message with a link to a website that installs malicious software.

Recognition (Example 2)

DO NOT LOGIN WITH YOUR INFORMATION IF YOU HAPPEN UPON A SIMILAR LOGIN SPOOFING PAGE

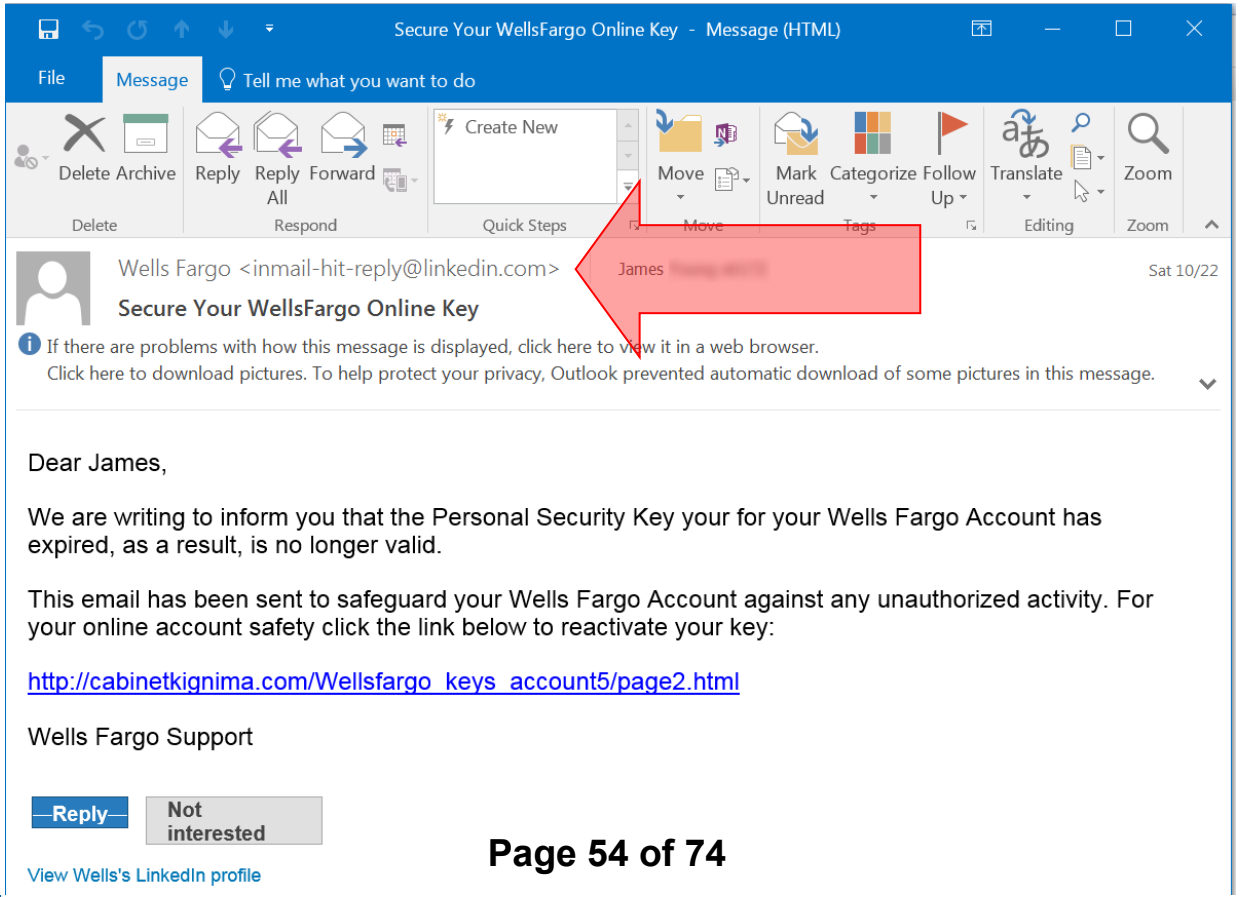


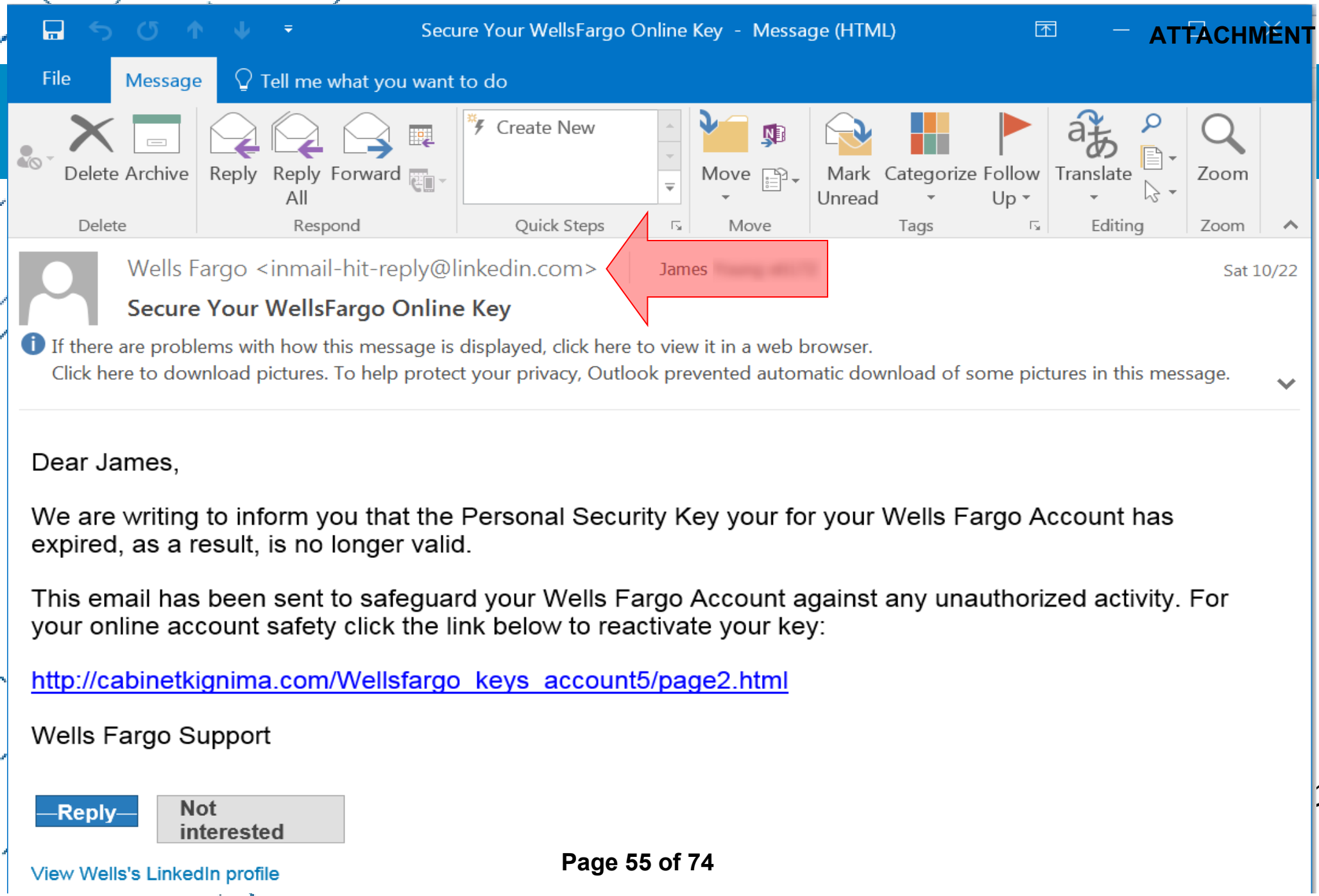



File:///C/Users/bobgeorge/appdata/local/googlephish.html
Google
One account. All of Google.
Sign in to continue to Gmail
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help
English (United States)

Recognition (Example 3)

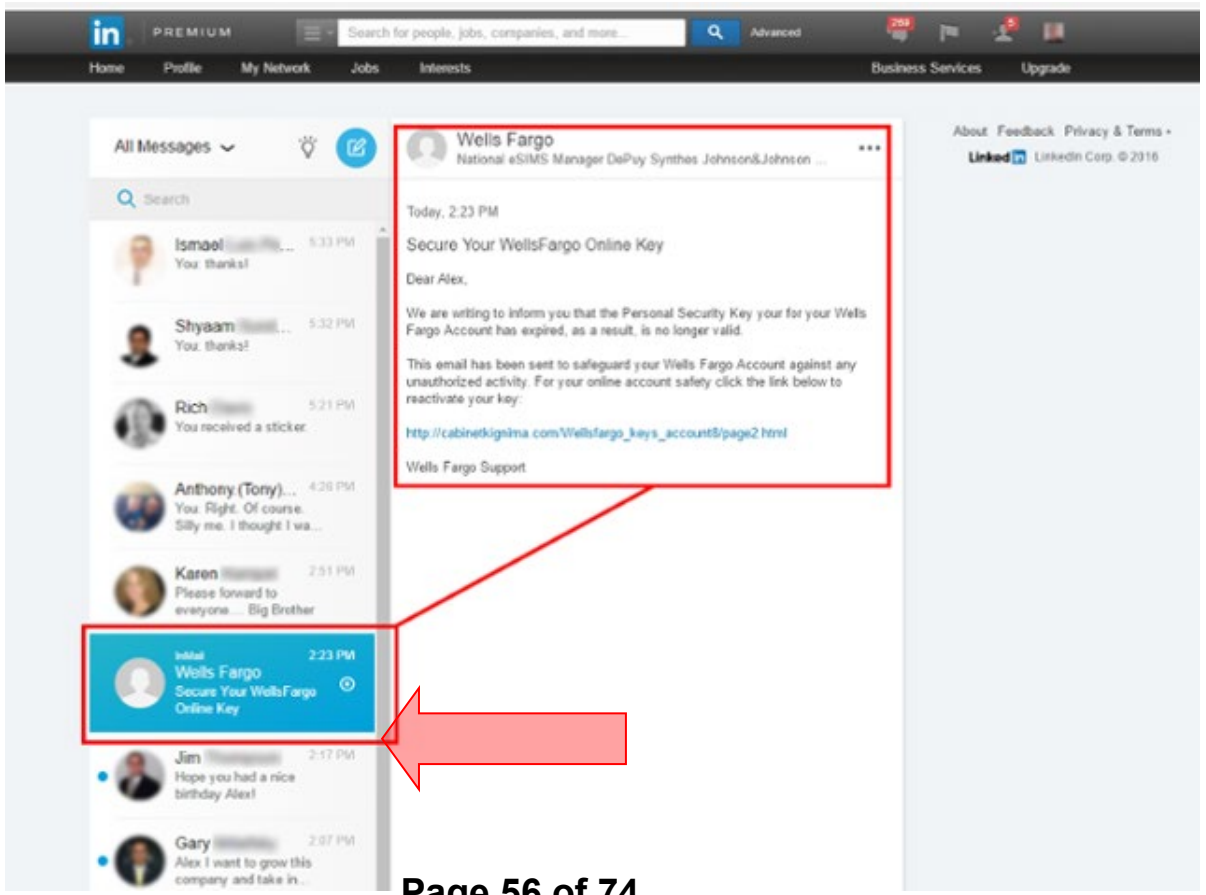
Example of a message with a Link that contains malware.
DO NOT OPEN IF YOU RECEIVE A SIMILAR EMAIL

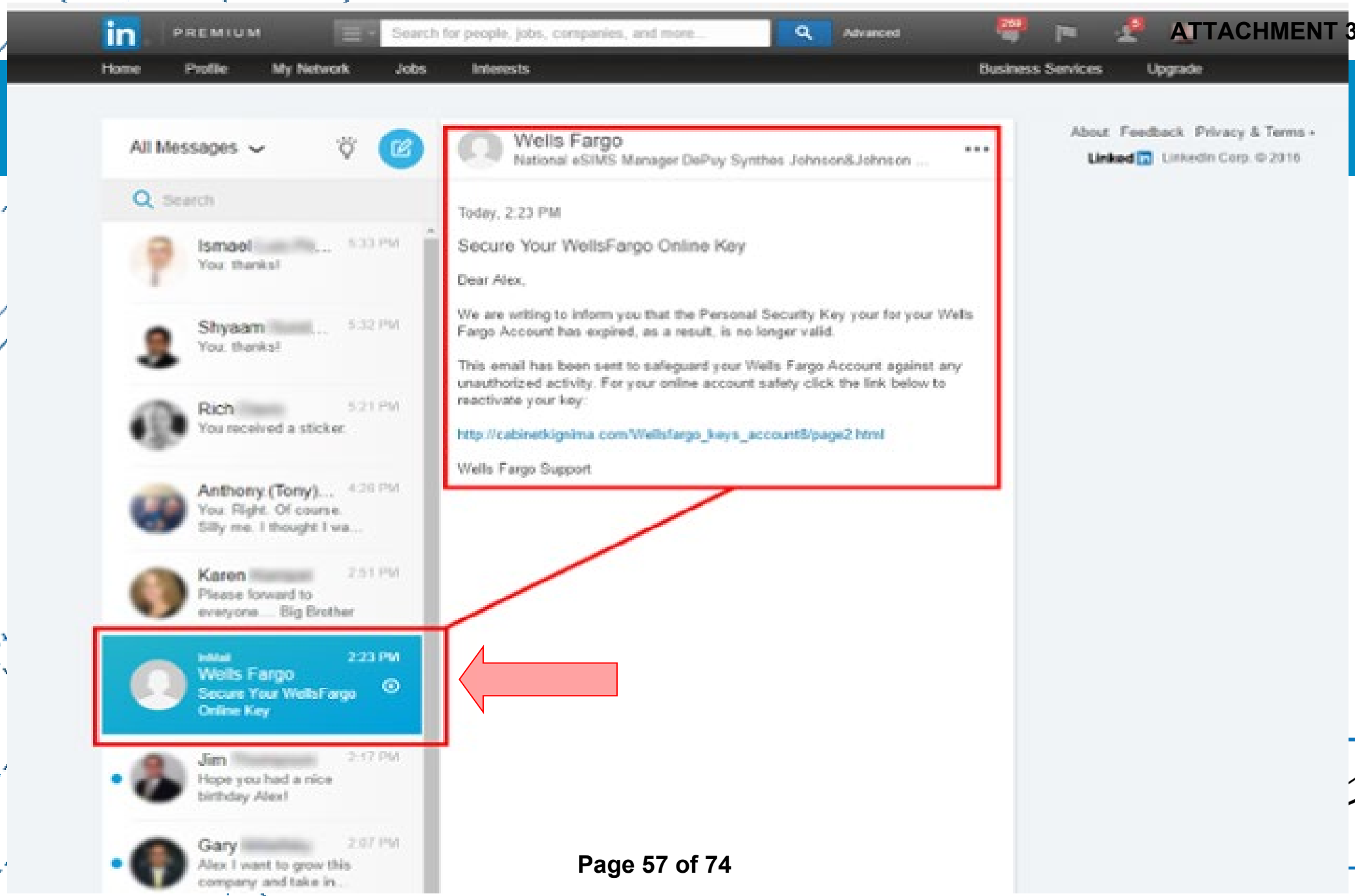



Secure Your WellsFargo Online Key - Message (HTML)
File
Message
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Wells Fargo <inmail-hit-reply@linkedin.com>
James
Sat 10/22
Secure Your WellsFargo Online Key
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Dear James,
We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.
This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:
http://cabinetkignima.com/Wellsfargo_keys_account5/page2.html
Wells Fargo Support
Reply
Not interested
View Wells's LinkedIn profile

Recognition (Example 4)

Example of a message with a LinkedIn message link that contains malware.




PREMIUM
Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Business Services
Upgrade
All Messages
Search
Ismael
You: thanks!
Shyaam
You: thanks!
Rich
You received a sticker
Anthony (Tony)...
You: Right. Of course.
Silly me. I thought I wa...
Karen
Please forward to
everyone.... Big Brother
InMail
2:23 PM
Wells Fargo
Secure Your WellsFargo
Online Key
Jim
Hope you had a nice
birthday Alex!
Gary
Alex I want to grow this
company and take in...
Wells Fargo
National eSIMS Manager DePuy Synthes Johnson&Johnson ...
Today, 2:23 PM
Secure Your WellsFargo Online Key
Dear Alex,
We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.
This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:
http://cabinetkigsima.com/Wellsfargo_keys_account8/page2.html
Wells Fargo Support
About
Feedback
Privacy & Terms
LinkedIn Corp. © 2016

Protect Yourself: Refuse the Bait

- Be cognizant and vigilant of this threat.
- Before clicking on any web link within a message or opening up an attachment, be sure the source of the email is legitimate.
- The links and attachments can contain:
  - Malware
  - Spyware
  - Viruses
  - Trojan horses
- STOP. THINK.
  - Before you click, look for common baiting tactics
  - If the message looks suspicious or too good to be true, treat it as such

Specific Examples

Date	Recipients	Subject	Sender	Detected By
10/21/19 12:27 PM	[redacted]chwell@dcyf.wa.gov	Undeliverable: Update Contact ...	[redacted]gov	Malicious URL reputation
10/21/19 12:30 PM	[redacted]chwell@dcyf.wa.gov	Undeliverable: Update Contact ...	[redacted]gov	Malicious URL reputation
10/21/19 1:03 PM	[redacted]astvaleca.gov	Your Miami Community News: ...	[redacted]apers.co...	Anti-spoof: external domain
10/21/19 1:03 PM	[redacted]stvale@gmail.com	Your Miami Community News: ...	[redacted]apers.co...	Anti-spoof: external domain
10/21/19 1:04 PM	[redacted]a@eastvaleca.gov	Update Contact Details for Dire...	[redacted]va.gov	Malicious URL reputation
10/21/19 1:05 PM	[redacted]chwell@dcyf.wa.gov	Undeliverable: Update Contact ...	[redacted]gov	Malicious URL reputation
10/21/19 1:12 PM	[redacted]chwell@dcyf.wa.gov	Undeliverable: Update Contact ...	[redacted]gov	Malicious URL reputation
10/21/19 1:16 PM	[redacted]eastvaleca.gov	Update Contact Details for Dire...	[redacted]va.gov	Malicious URL reputation
10/21/19 1:42 PM	[redacted]a@eastvaleca.gov	REMINDER: Join Us On 11/2 For...	[redacted]cities.org	Anti-spoof: external domain
10/21/19 3:00 PM	[redacted]astvaleca.gov	CESA	[redacted]	Advanced phish filter
10/21/19 5:56 PM	[redacted]s@eastvaleca.gov	schd inspection for Wednesday ...	[redacted]	Anti-spoof: external domain
10/21/19 8:36 PM	[redacted]@eastvaleca.gov	DC Comics prop; Hamburger Bu...	[redacted]om@p...	Anti-spoof: external domain
10/21/19 9:28 PM	[redacted]eastvaleca.gov	Today's Local Government New...	[redacted]	Anti-spoof: external domain

Got Hooked?

If you suspect…	You should…
You interacted with or replied to a phishing scam using your Work email account	Immediately contact the Interwest IT Help Desk:
You might have revealed or shared personal or financial information	Immediately change the password(s) for your account(s). If you use the same password for multiple accounts and sites, change it for each account. Do not reuse that password in the future. Watch for signs of identity theft by reviewing your bank and credit card statements for unauthorized charges and activity. If you notice anything unusual, immediately contact your credit card or bank. Consider reporting the attack to the police, and file a report with the Federal Trade Commission: www.ftc.gov.

Viruses and Malware

- Cybercriminals also use attachments to spread viruses or other malicious software (malware) to steal or destroy data.
- Malware can install keyloggers to capture everything you type, control your webcam/microphone, or send all of your data to remote servers that the criminal controls.
- The attachment typically arrives as Word, Excel or PDF file and has to be opened before the malware triggers.
- Malware will take advantage of unpatched software.
- Some Word/Excel malware require you to enable Macros – always be suspicious of an attachment that requests you to “lower” your security settings when opening.

Ransomware

- Ransomware is a new type of malware that encrypts documents, pictures and other files, making them unreadable. The attacker then holds the decryption key for ransom until you agree to pay money, usually through an untraceable method such as BitCoin or other digital currency.
- Ransomware assumes that you'll pay to recover your files – if you back them up regularly, you have no need to pay the ransom.
- On City machines, store files on your network drives, OneDrive, etc. At home, use external drives or trusted cloud services.

Encryption: A Key Component of Ransomware

- Ransomware, in its most basic form, is self-explanatory. Data is captured, encrypted, and held for ransom until a fee is paid. The two most common forms of ransomware delivery are through email and websites.
- Ransomware has been continuously evolving in the past decade, in part due to advances in cryptography. The wide availability of advanced encryption algorithms including RSA and AES ciphers made ransomware more robust. While estimates vary, the number of ransomware attacks continues to rise.

Ransomware on the Rise

- Bitcoin has been a significant factor in the rise in ransomware attacks. The lack of oversight by any governing body coupled with anonymity makes it an ideal currency in ransomware demands.
- The evolution of ransomware-as-a-service (RaaS) has also played a significant role in the proliferation of attacks. RaaS has moved the execution of a ransomware attack from "professional" to "script-kiddie."
- Operating systems lack runtime detection capabilities that could help stop ransomware execution in the early stages possibly even before actual encryption begins.

Recent Victims of Ransomware Attacks

- June 26, 2019: Lake City, Florida agrees to pay ransomware.
- June 20, 2019: Riviera Beach, Florida, discloses ransomware attack and payment.
- May 7, 2019: City of Baltimore hit with ransomware attack.
- April 2019: Cleveland Hopkins International Airport suffered a ransomware attack.
- April 2019: Augusta, Maine, suffered a highly targeted malware attack that froze the city's entire network and forced the city center to close.
- April 2019: Hackers stole roughly $498,000 from the city of Tallahassee.
- March 2019: Albany, New York, suffered a ransomware attack.
- March 2019: Jackson County, Georgia officials paid cybercriminals $400,000 after a cyberattack shut down the county's computer systems.

In the Event of a Ransomware Attack

- While these practices are effective, it is impossible to completely protect your organization from ransomware. If you do believe you have been the victim of a ransomware attack, consider the following steps:
- **Shut down your system. Physically unplug it if necessary.**
- **Notify IT ASAP**.
- The faster IT is notified the faster the spread of the ransomware can be stopped.

Social Engineering – Phone Scams

Phone call scams vary in their approach:

- Claim to be reputable businesses needing access or information

  "…this is Microsoft calling to let you know we have seen malware on your computer… can you help us get remoted in to your computer to get it removed for you…"

- Often convince you to provide information to "verify" you

  "…your illegal browsing web history has been logged and will be reported to the authorities if you do not provide your social security number to prove who you are…"

- Claim interruption of service or other negative consequences if you don't comply

  "…there is a billing issue with your account, can you please provide your credit card number for verification, otherwise services will be disconnected immediately…"

Social Engineering

Be aware of possible social engineering

1. Phone calls from unknown/unverified sources
2. USB drives from non-reputable sources or just lying around on a desk or table
3. CD/DVDs from non-reputable sources
4. Plugging in non-work phones/other devices
5. Password or login requests
6. Threatening or urgent abnormal requests
7. Requests for large sums of money
8. Co-workers acting strange over email

Password Tips

- Keep your password complex
- Change your password regularly
- Never share your password! Even with a coworker or vendor
- Never write down or email your password
- If you believe your password may be compromised change it immediately and report it!

Password Complexity Live Demo

- https://password.kaspersky.com/

Password Complexity

Pattern	Calculation	Result	Time to Guess ($2.6x10^{18}$ tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	$5x10^5$	
8 chars: lower case alpha	26^8	$2x10^{11}$	
8 chars: alpha	52^8	$5x10^{13}$	
8 chars: alphanumeric	62^8	$2x10^{14}$	3.4 min.
8 chars alphanumeric +10	72^8	$7x10^{14}$	12 min.
8 chars: all keyboard	95^8	$7x10^{15}$	2 hours
12 chars: alphanumeric	62^{12}	$3x10^{21}$	96 years
12 chars: alphanumeric + 10	72^{12}	$2x10^{22}$	500 years
12 chars: all keyboard	95^{12}	$5x10^{23}$	
16 chars: alphanumeric	62^{16}	$5x10^{28}$	

Other Safety Tips

- Stay away from "Free" music/movie download sites as they generally contain malware disguised as media content.
- Practice safe web browsing habits by staying away from:
  - Social media links
  - Advertisements
  - Email links that are unfamiliar to you,
  - Even if from known sources, THEY MAY BE COMPROMISED.
- Limit web browsing to:
  - Work related sites only
  - No personal email
  - No browsing on work computers

Other Safety Tips

Lock computer when walking away

Always escort unknown guests

Never leave guests unattended within reach of technology or sensitive material

Report suspicious emails/calls/incidents

STOP and THINK before you CLICK!

Thank you!