Ransomware....
A discussion of how it can impact your business and ways to protect yourself from contracting it!

How can Link’s Managed Service secure your environment?
If you are not preparing your organization for the growing need for cyber-security and prevention, it's something that needs to move up your “to-do” list.

This session will provide case studies of real world (and very recent) cyber-crime events within Pennsylvania businesses, including the “costs” of the crime, what it took to recover from the events, and what could have been done to prevent them from happening to begin with.

If you are not familiar with the terms of “phishing” and “ransomware”...you need to be. This session will help provide you an understanding of these and other terms, plus how important cyber-security, layered prevention and employee education are to every organization.

Ransomware

**What is Ransomware**

- A malicious program that purposefully encrypts all your user files, which means that unless you pay the ransom, or you have a recent backup, your files are gone forever
- It holds your data/network hostage to attempt to extort a ransom payment
How the Ransomware gets on your network:

- Open an email with an infected attachment
- (great uncle...holiday package notices..etc.)
- Click on an advertisement that contains ransomware
- Going to an infected website
- Click the wrong link

What Happens?

- Malicious Software or Virus contained within gets attached to the individual machine(locally)
- Then attaches its tentacles to all your connected (mapped) drives and locks you out with that infamous screen shot we just viewed

PHISHING = FAKE EMAIL BUT LOOKS REAL!

- Phishing: a supposed ‘trustworthy entity’ asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.

Dear Chase Customer,

As part of our commitment to help keep your account secure, we have detected an irregular activity on your account and we are placing a hold on your account for your protection.

Please click the link below and follow the instructions to unlock your account.

[Online Banking Log-in Restore]

We are here to assist you anytime. Your account security is our priority.

Thank you for choosing Chase Bank.

Sincerely,

Chase Fraud Department
--- Original Message ---
From: Dawn <contact3@mygrafik.com.gr>
Sent: Wednesday, April 24, 2019 12:10 PM
To: Mandy
Subject: Your Dawn Flower order has shipped

Dear Mandy,

Please see below:

https://siriusco.com/617a-9952hk9-sf9k2h52f8e-92q-952h0-key:1242c1e12-591292f58214-42959-3181942x134

Thank you in advance

Dawn

Mail: 290-730-4796 Fax: 290-730-4754
E-Mail: contact3@mygrafik.com.gr

--- Fake Email Example ---

From: Watts Jerrold@mittelstad.com
To: invoices@mittelstad.com
Subject: Invoices
Size: 5931
Source IP: unknown [160.169.84.234]
ID: 148112612-09989388398818001-ExpCzK

View Message View Source View Bayesian Data

Charset: utf-8

Dear,

By today, three invoices (4282, $284, $4283, $959, $4287, $564) are not paid. Starting tomorrow, fines will be charged. Please make appropriate payments.

All details are in the attachment.

---

Best Regards,
Jerrold Watts
Sales Director

invoices5756069.zip (5)
Protect Your Data from Ransomware!

• A good defense uses multiple layers of offense to address technical, personnel and operational issues
• Install a firewall as it acts as a wall between your computer/private network and the internet and filers packets that enter and leave your network. A firewall prevents hackers from entering your computer.
• Install Anti-virus software…it detects malware and can destroy it before any damage is done
• Protect Your Operating System…. Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
• Create a good strong passwords and perform password management routinely
• Do not open email attachments that you know are garbage….Cultural Awareness!
• Do not click on links in emails unless you are absolutely sure of their validity.
• Only visit and/or download software from web pages you trust.
• Use Encrypted email services for sensitive information
• Backup….could be the most important….how often do you backup?? Is your backup part of a disaster recovery plan? Do you have a redundant offsite secure copy? How often do you test your backup? Is it encrypted?

PUT THIS KNOWLEDGE TO WORK!

• These are only some of the best practices involving Information Security.
• Use these practices at home and at work to keep your data and intellectual property safe and secure.
• Most employers have policies and procedures regarding secure practices for their data and networks. If you don’t you may want to establish them. Be sure to understand the policies and procedures and adhere to them. It will protect you, your employer, its intellectual property and last but not least it will help protect your customers.
• If in doubt, ask someone, including Your IT Help Desk if you’re not sure about the legitimacy of an email, program, pop-up, or other strange window or message on your PC.
QUESTIONS?

Presenters

Tim Serbin, tserbin@linkcorp.com
Tim is and Account Manager who specializes in managed services dealing with network security/compliance, virtualization, backup, disaster recovery, business continuity and cloud communications/collaboration. His years of experience allows him to connect with all businesses including municipalities, professional practices such as medical, legal, accounting as well as manufacturing industries to provide efficient technology solutions enabling his customers to maximize the return on their IT investments as well as preventing costly down time and service interruptions.

Derek McLaurin, dmclaurin@linkcorp.com
Derek is the Director of Design and Strategy at Muni-Link. He has over 40 years of Information Technology experience having spent the last 10 years focusing on municipal government organizations across the country. Derek has industry background in Utility Billing, Finance, Customer Information Systems, Customer Communications, and Municipal Websites. He also has involvement specifically in the municipal field having served as a Borough Councilman, the Borough Fire Chief, and the Water Authority Board Vice Chairman.

Jim Rokosky, jrokosky@muni-link.com
Jim joined Muni-Link in 2019 and brings 25 years of product development and operations experience to his role as the SVP of Operations. Jim’s experience is complimented by a Bachelor of Science in Electrical Engineering from Penn State University, a Master of Science in Software Engineering from Monmouth University, and various executive level courses from the Penn State Smeal College of Business. Jim holds several US patents in the software and technology field. As Vice President of Operations at Muni-Link, Jim is responsible for Software Development, Quality Assurance, Implementations and Customer Support.

Jim joined Muni-Link in 2019 and brings 25 years of product development and operations experience to his role as the SVP of Operations. Jim’s experience is complimented by a Bachelor of Science in Electrical Engineering from Penn State University, a Master of Science in Software Engineering from Monmouth University, and various executive level courses from the Penn State Smeal College of Business. Jim holds several US patents in the software and technology field. As Vice President of Operations at Muni-Link, Jim is responsible for Software Development, Quality Assurance, Implementations and Customer Support.

Jim joined Muni-Link in 2019 and brings 25 years of product development and operations experience to his role as the SVP of Operations. Jim’s experience is complimented by a Bachelor of Science in Electrical Engineering from Penn State University, a Master of Science in Software Engineering from Monmouth University, and various executive level courses from the Penn State Smeal College of Business. Jim holds several US patents in the software and technology field. As Vice President of Operations at Muni-Link, Jim is responsible for Software Development, Quality Assurance, Implementations and Customer Support.