Security Best Practices and Planning for Tomorrow’s Internet
CMJ is a provider of IT services to businesses and nonprofit organizations throughout Northern Illinois.

Over 20 years of technology experience and expertise.

Founded in 2007

A life-long DeKalb County Resident
Security & Best Practices

Identify and define common security threats

Best practices for protecting yourself and your organization against them
1. Who is it OK to share passwords with?

A. Your boss
B. Human Resources
C. Your Co-worker
D. Close friends or family
E. None of the above
2. What should you do to close an unwanted pop-up window?

A. Click the “Ok” or “Close” button
B. Click the “X” in the corner of the window
C. Press Alt + F4
3. True or false. If you use a public Wi-Fi network (in a café or hotel, for example) that assigns you a password, it’s okay to send confidential business data.

True                      False
4. What tips should you follow when opening attachments or links?

A. If a message comes from someone you know personally, it’s okay to open or click them.
B. Make sure your antivirus software is up to date.
C. Don’t open or click links if they appear out of context – for example: ilovepinkpinies.pdf from your boss.
D. Look carefully at the link or attachment to see if it’s safe to open.
E. View every one with suspicion.
5. What percentage of US adults had their information hacked between 2013 and 2014? Hacking may include accessing emails, stealing identity, installing malware, etc.

A. 5%
B. 10%
C. 20%
D. 50%
E. 75%
6. How can you tell if an email is fraudulent?

A. Unfamiliar email address
B. Alarmist messages urging you to take action as soon as possible
C. Grammatical errors
D. Account-related requests, such as asking for login information or passwords
E. All of the above
7. True or false: If you’re using Windows XP or Office 2003 you are receiving regular security updates.

<table>
<thead>
<tr>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8. What can you do to strengthen your software defenses?

A. Keep software up to date
B. Install automatic updates when offered
C. Install antivirus software
D. Protect your router with a password
E. All of the above
9. How can you be sure your sensitive data is encrypted?

A. It’s safe as long as you use a private WiFi network.
B. Purchase data encryption services.
C. Use a device or operating system with built in data encryption, such as Windows 10.
D. Use only apps from trusted developers.
E. Send information over cellular data rather than WiFi.
10. Of people who were victims of online fraud, the average financial loss was between:

A. $0 - $500
B. $1000 - $5000
C. $5000 - $10,000
D. $10,000 +
Security Threats

- Phishing
- Spam
- Viruses
- Ransomware
Email designed to impersonate a person or company. Used to obtain sensitive information such as passwords, account numbers, social security numbers.

Common characteristics:
• Disguised links
• Incorrect domain in sender’s email address
• Poor punctuation or spelling
• Generic information about you
Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates
Dear Visa customer,

This email is to inform you of a recent update we made to our systems. To avoid service interruption we require that you confirm your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

http://visa-secure.com/personal/secure_with_visa/

Follow these steps:

1. Confirm your account by clicking the link above.
2. Verify your visa card information.
3. Your account will then be updated, you may continue using your visa without any issues.

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

We apologize for any inconvenience this may cause. The visa team is working hard to bring you the best services on the web.
Process a wire of $357,493.41 to the attached account information. Let it be coded admin expense. Send me the confirmation when completed.

Thanks
Tim

-------- Forwarded message --------
From: Kemp, Tom <tom.kemp@centrify.com>
Date: Feb 12, 2014
Subject: Wiring Instruction
To: Timothy.Steinkopf@centrify.com

Tim,

Per our conversation, attached is the wiring instructions for the wire. I’ll send the documentation later on. Let me know when done.

Thanks
Tom
Unsolicited commercial email that can be malicious in nature

Waste of employee time and company resources

May carry viruses – be wary of attachments
   - If you don’t know the sender, don’t open an attachment

For legitimate companies, unsubscribing may help, for illegitimate companies, it can have the opposite effect
The unintentional downloading of malware in a browser, i.e. Google Chrome. Most often this is caused by:

- Visiting a malicious website
- Clicking a bad link in a phishing or spam email
- Mistyping a URL (website address)

Causes the browser to download and possibly execute a virus-like file, often without the users consent or knowledge, infecting the device in the background.
Viruses

One vulnerable PC can infect a network
Can take different forms and intrude in different ways
Used to attack your computer or spy on you
Ransomware

Most recent high profile security threat, emerged within the last 5 years, e.g., WannaCry – May 2017

A malicious program that encrypts your data so that it is no longer accessible to you and then demands a ransom in order to decrypt the data.

Encrypts all files on your computer and any shared folders you have access to.

Once a computer is infected, the infection can spread to other computers on the network.

DATA CANNOT BE DECRYPTED WITHOUT PAYMENT!
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

[Bitcoin address]

[Payment buttons] Check Payment

[Decryption button] Decrypt

[Links]
About bitcoin
How to buy bitcoins?
Contact Us
Best Practices

The steps you can take to protect your network, hardware and data.
Anti-Virus Software

Anti-virus software that has real time protection that is monitored is preferred.

Microsoft includes basic protection in Windows 8 and higher.

Automatic updates of virus definitions.

More advanced or additional software may be available from your internet provider or local reseller.

Web Filtering may be available as an additional add-on or may be included with your firewall and can help prevent viruses by blocking known malicious sites.
It is critical your OS and software are up to date at all times. Most often viruses and malware are targeting vulnerabilities that exist and have not been patched.
Your passwords are the first line of defense for access to your accounts and networks.

Implement a password policy

- Make sure you have strong passwords
- Have strong password reset questions
- Use a unique password for each site
Use Secure Passwords

- Avoid using the same password for multiple sites/computers
  - Randomly generated passwords
  - Long combinations of letters, numbers, symbols or a long phrase that’s easy to remember

- Employ the use of a Password Manager

- There are several free or low cost password managers available. Examples are LastPass, 1Password, Enpass.
Two Factor Authentication

With this, a user has to confirm their identity using a combination of two different methods.

A good example of this would be logging into your bank account and not only providing your password, but also a PIN that is sent to your mobile device.
Backups are Important
Backups

Backing up your data is the first step and best insurance you have for your organization and your peace of mind.

- Do you know how often your data is backed up?
- What is being backed up?
- Do you know what backup software you are using?
- Are they automated or is it a manual process?
- Have the backups been completing successfully?
- Do you have local, offsite or both?
- Have you done a trial or test restore?
- How secure are they?
The best security can’t be passive, it must be actively maintained to adapt to emerging threats.

Raising employee awareness is also a great way to make sure your staff understands the importance of security.

Provide annual or frequent employee training on topics such as:

- How to identify suspicious emails, files, websites, etc.
- How to select a strong password

Designate an employee or consultant to be responsible for security and data protection implementation and maintenance.

Lock your computer when you walk away.
THANK YOU

Chad Jewett
chad@cmjtech.net
815-899-2468
www.cmjtech.net