

<http://www.jeffersoncountywi.gov>


How QR Codes

Hide privacy and security risks

QR codes, those little black-and-white puzzle-like square matrixes that increasingly populate ads and promotional posters, are meant to provide smartphone users with product details. But trusting consumers who scan these squares and comply with permission requests could get more than they bargained for in the way of security and privacy problems.

But experts say all this swiping could cause some security, and perhaps privacy, issues for unsuspecting users. The QR code itself can link to malicious text messages or malicious websites, said Tim Armstrong, a malware researcher at the international anti-virus firm Kaspersky Lab.

"Unfortunately, this is a case of buyer beware," Armstrong said. "Being that this is a new territory, be suspicious of everything. If you are walking through town and see a QR code on a local real-estate office, there's a small chance of being infiltrated, but if you are visiting a Russian website, you have a much larger chance of being infected."

"Understanding your device, the QR app, how it interacts with URLs, and how permissions are granted with your mobile OS are important."

- *SecurityNewsDaily, 2012*
- <http://www.technewsdaily.com/>



October is Cyber Security Awareness Month ...From the desk of RW P.5

In this issue

Where is your personal data? P.1

WiFi: Connect with Care... P.2

Outlook 2010 Shortcuts P.3

Easy to use Security Tips... P.4

...From the desk of RW P.5

Do You Know Where Your Personal Information Is?

The amount of data on the Internet is staggering...

As consumers of online services, we create information through our use of social media, online shopping, and many other activities. Public records are also a source of information about individuals, which can get posted online.

It is important to be aware that once this data is online, that can be difficult to remove.

Clean up the data you can control

Review the accounts that you have access to. You basically have three options—remove the data, modify the privacy settings, and/or request that the account be deleted. If you are going to request that the account be deleted, be sure to first remove all of the data. Be sure to request that the account be deleted rather than deactivated.

Request cleanup of data you don't control

Contact site owners. If the site does not have contact information for the site owners easily visible, you can look it up using the "WHOIS" service to give you an administrative and technical contact for the site. A "WHOIS" query can be done by visiting the website <http://whois.net/>.

Opt out of data service providers. The data service provider is a company or group that will provide lists of contact information to individuals or companies that request it. They often charge a fee for this information.

The best course of action that you can take is to be aggressive about maintaining a cycle of checking your public data and removing items which don't match your current risk tolerance.

—MS-ISAC, May 2013

...From the desk of
**John Rageth, MIS Systems
and Application Manager**



Public Web Page Transfer

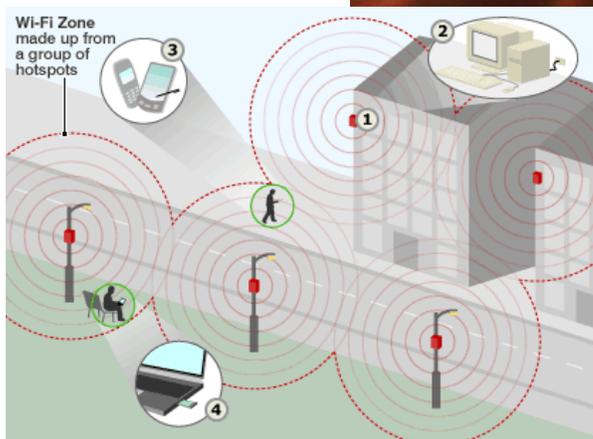
The Jefferson County Public Page is going to be hosted off site. We have contracted with **Revize**, a web hosting and **Content Management System** (or CMS) company.

Revize offers several advantages to the county:

1. Provides an extra layer of protection for disaster recovery. The website would still be available for communication if something happened to our other servers.
2. Content Management System (CMS) has history logs so that changes made to the site can be reversed or at least checked.
3. There are several backups of the website; this redundancy helps maintain performance if there are server or security issues.

The site framework has been prepared by Revize. Currently Tammie Jaeger and the MIS department are converting all the current pages to Revize (CMS). Once this task is completed, all of the individual department website administrators will be trained on the new CMS.

The site should go live in early 2014.



Wi-Fi: Connect with Care....

If you're traveling this summer, chances are you'll encounter a Wi-Fi hotspot (network) or two. Wi-Fi in airports, hotels, train stations, coffee shops, and other public places can be convenient, but they're often not secure, and can leave you at risk.

Whether you're entertaining the kids by streaming a video on a tablet, downloading new travel apps on your smartphone or even taking your tablet poolside, there are precautions you should take to make sure your personal information is safe.

First and foremost, connect with care. If you're online through an unsecured network, you should be aware that individuals with malicious intent may have established a Wi-Fi network with the intent to eavesdrop on your connection. This could allow them to steal your credentials, financial information, or other sensitive and personal information. It's also possible that they could infect your system with malware. Any free Wi-Fi should be considered to be "unsecure." Therefore, be cautious about the sites you visit and the information you release.

Access to paystubs from home....

MIS has been working on allowing employees to once again access their paystubs online. We have had several employees request this feature. It has taken some time to work through the needs for access with making sure all the security concerns are answered.

The new paystub system will allow employees to use the current login credentials from the employee site. The system will show all the financial information of the current paystub, however all the personal information will be redacted. This redacted information includes name and address of employee.

The employee will be able to see the last three paystubs online. If an employee requires older stubs or needs a stub with their name and address on it, they can use the current employee site, or if they don't have access to a county computer they can request paystubs from payroll. This new access will be in place in December.

—JFR

STOP. THINK. CONNECT.

Here are 6 tips to remember when using Wi-Fi:

- (1) Keep an updated machine. Having the latest security software, operating system, web browser and apps can help protect you from the malware and other threats you may encounter when using Wi-Fi.
- (2) Don't assume that the Wi-Fi connection is secure. Many hotspots don't encrypt the information you send on the Wi-Fi network.
- (3) Do not log into accounts, especially financial accounts, when using public wireless networks.
- (4) Do not log onto sites that don't seem legitimate, (clues could include the URL being misspelled, or not matching the name that you were given by the place of business). It's not uncommon for cybercriminals to set up a Wi-Fi network called "free Wi-Fi" in airports, hotels, and other public places.
- (5) A cellular 3G/4G connection is generally safer than a Wi-Fi connection.
- (6) Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi.

— MS-ISAC, July 2013

(See more at their website; <http://msisac.cisecurity.org/>)

EYE ON IT

Mobile Threats Are Increasing

Smartphones, or mobile phones with advanced capabilities like those of personal computers (PCs), are appearing in more people's pockets, purses, and briefcases. Smartphones' popularity and relatively lax security have made them attractive targets for attackers. According to a report published earlier this year, smartphones recently outsold PCs for the first time, and attackers have been exploiting this expanding market by using old techniques along with new ones. The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up.

Smartphones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation, and many other applications. However, smartphone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers.

Unfortunately, many smartphone users do not recognize these security shortcomings. Many users fail to enable the security software that comes with their phones, and they believe that surfing the internet on their phones is as safe as or safer than surfing on their computers. Meanwhile, mobile phones are becoming more and more valuable as targets for attack.

— US-CERT, 2011 (www.us-cert.gov/)



Microsoft® Office 2010

Common Outlook 2010 Procedural Shortcuts....



For more **Outlook 2010 Shortcuts**, check out this link; <http://office.microsoft.com/en-us/outlook-help/keyboard-shortcuts-for-microsoft-outlook-2010-HP010354403.aspx>

Google Chromebook trial underway for Jefferson County Board members

As a pilot program established by the Jefferson County Board and Jefferson County MIS, three board members volunteered to try out three Google Chromebooks acquired by MIS to test the viability of these devices for County Board use.

County Board members Augie Tietz (District 4), Amy Rinard (District 9), and Jim Schroeder (District 19) all volunteered to try out the three trial Chromebooks to analyze how they would work for County Board meetings and functions.

The idea for this trial started with board Supervisor John Molinaro as a means to allow for County Board members to access meeting agendas, minutes, and other data needed for committees. Hopefully some money might also be saved to reduce paper and copying costs as well.

The trials continue with these new devices to understand how they will or will not work in our County Board environment.

—STK/ MIS

(Special Thanks to Nathan Mott at pandodaily.com for the graphic above)



TO DO THIS	PRESS
Switch to Mail.	CTRL+1
Switch to Calendar.	CTRL+2
Switch to Contacts.	CTRL+3
Switch to Tasks.	CTRL+4
Switch to Notes.	CTRL+5
Switch to Folder List in Navigation Pane .	CTRL+6
Switch to Shortcuts.	CTRL+7
Switch to next message (with message open).	CTRL+PERIOD
Switch to previous message (with message open).	CTRL+COMMA
Move between the Navigation Pane , the main Outlook window, the Reading Pane , and the To-Do Bar .	CTRL+SHIFT+TAB or SHIFT+TAB
Move between the Outlook window, the smaller panes in the Navigation Pane , the Reading Pane , and the sections in the To-Do Bar .	TAB
Move between the Outlook window, the smaller panes in the Navigation Pane , the Reading Pane , and the sections in the To-Do Bar , and show the access keys in the Outlook ribbon.	F6
Move around message header lines in the Navigation Pane or an open message.	CTRL+TAB
Move around within the Navigation Pane .	Arrow keys
Go to a different folder.	CTRL+Y
Go to the Search box.	F3 or CTRL+E
In the Reading Pane , go to the previous message.	ALT+UP ARROW or CTRL+COMMA or ALT+PAGE UP
In the Reading Pane , page down through text.	SPACEBAR
In the Reading Pane , page up through text.	SHIFT+SPACEBAR
Collapse or expand a group in the email message list.	LEFT ARROW or RIGHT ARROW
Go back to previous view in main Outlook window.	ALT+B or ALT+LEFT ARROW
Go forward to next view in main Outlook window.	ALT+RIGHT ARROW
Select the InfoBar and, if available, show the menu of commands.	CTRL+SHIFT+W



Easy to Use Security Tips.....

Do not write your password down and leave it near your computer

Writing your password on a 'sticky-note' and sticking it on your monitor makes it very easy for people who regularly steal passwords to obtain yours. Hiding it under your keyboard or mouse pad is not much better, as these are common hiding places for passwords. However if you must write something down, jot down a hint or clue that will help jog your memory or store the written password in a secure, locked place.

Do not allow Internet Explorer (IE) to store passwords for you

Stored passwords allow anyone who can access your machine to log in to your web accounts as you. In addition, there are numerous utilities that can expose that hidden information and actually reveal the password. If you've reused that password for other logins, many systems or web sites could be compromised.

If you get up from your computer, lock it! *Ctrl+Alt+Delete*, then hit *Enter* at your Keyboard to lock your PC or Laptop

Don't tell anybody your password

This warning includes your systems administrator, who **NEVER** needs your password. One day an e-mail was received from what looked to be a legitimate address saying they needed my password for maintenance, and if you did not go to a webpage and give it to them, they would suspend the account. As it turns out, I'm the one in charge of "waidele.info" — so I'm the one who gives out accounts and does maintenance. Things might have ended differently if we had an account with googlemail.com or aol.com. Then the senders would have called themselves "support@aol.com" causing the user to be fooled .

EYE ON IT

Cops To Apple Users: Please Update To iPhones and iPads to iOS 7

Apple's new operating system makes it far more difficult to reprogram a stolen iPhone or iPad thanks to a feature called Activation Lock. In the event of loss or theft, the feature requires your Apple ID and password to reactivate the phone. Since most thieves aren't likely to have that information at hand, stolen iPhones should be effectively bricked, and therefore worth much less .



Police departments and law enforcement officials like

anything that might make iPhone theft—now dubbed "Apple picking"—less lucrative. So they're calling on all iPhone and iPad users to upgrade to iOS 7 as soon as possible.

Apple is clearly taking security threats seriously. The new iPhone 5S that debuted last week has a fingerprint scanner to protect your identity, in addition to the lock code function that most phones already use.

The increased security protection will make it far more difficult for anyone to gain access to the iPhone, though many are already trying to find a way around it.

PLEASE UPGRADE through iTunes..

Read more at: <http://readwrite.com/2013/09/23/apple-ios-7-update-police-prosecutors-theft#awesm=~oitYGZggKnTrPR>

Rick's Tips (from the desk of Rick Christian, Senior Microcomputer Specialist)

Beware of USB flash drive's autoplay feature

If you find a USB token in the wild, don't plug it into your USB port as it could autoinstall software if your system is set to autoplay CDROMs.

Though many organizations' standards call for disabling autoplay of CDROMs, you should check and set yours. To disable autoplay follow these instructions (for WinXP):

Open My Computer

Right click on your CDROM drive selecting "Properties"

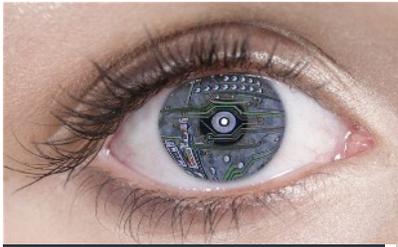
Select Autoplay page and set each menu option to "Select an Action to Perform" = "Take no action"

Click Apply (you must apply each setting change one at a time!)

Repeat for each item in the list (alternatively ensure that all are set to "Prompt me for action")

Thanks to: pulse2.com for this picture





EYE ON IT

Protect Yourself from Email Phishing Attacks

In the pre-Internet era, con men, also known as confidence men, would gain victims' confidence through the use of deception, to defraud them. One of the most prolific modern means for online scamming is phishing.

When using the Email, it is difficult to know, with certainty, with whom you are communicating. Scammers will utilize this uncertainty to pose as legitimate businesses, organizations, or individuals, and gain the trust of users.

Phishing scams are perhaps one of the best-known forms of email scams. The scammers will try to obtain the user's financial information using an empty promise of sharing the wealth in exchange for their help.

Spear-phishing is a targeted and personalized attack in which a specific organization or an individual is the target. These attacks will utilize information about the user email addresses and often requires a lot of information gathering on the targets and have become one of the favored tricks used in cyber espionage.

Thanks to MS-ISAC, April 2013

Check out these other resources:

FTC's Identity Theft Website:

www.ftc.gov/bcp/edu/microsites/idtheft

AntiPhishing Work Group:

www.antiphishing.org

....From the Desk of Roland Welsch, MIS IT Manager



Dropbox File Sharing Tips

File sharing sites such as **Dropbox** make it very easy to share files. They also make it very easy to be hacked. My first suggestion is: if you have data that is sensitive, be careful before putting it on a file sharing site such as this. If you do put it on a site like this, make sure you have a strong password that you change every 90 days.

Some file sharing services are starting to offer 2 factor authentications. If you have data that needs to be secure, you should enable 2 factor authentication when it becomes available.

If the site doesn't have plans for 2 factor authentication, then select another file sharing site that does offer this capability.

More information on this for Jefferson County employees will be coming after our 2013 MIS Security Audit is complete.



Thanks to Chelsea Lewis of WisconsinTrails.com for the picture on the left



Android Tips; Using Copy and Paste

A powerful yet completely hidden feature is easy to use once you find it.

The general process of using copy & paste is quite simple. Find the block of text that you'd like to copy, and do a long press on it. A menu will pop down from the top of the screen and you'll see small tabs and a highlight on the selected text appear as well. Drag the tabs to select the desired text you wish to copy, and look up to that new menu.

In the top bar, from left to right are options to select all text, copy selected text, share the selected text and perform a Google search on the selected text. The buttons aren't the most intuitive, but once you're used to what they do this copy & paste menu becomes quite useful. When you want to paste the text you copied, simply do another long press in a text field and select the "paste" option that pops up.

Read more at: <http://www.androidcentral.com/android-101-using-copy-paste>



Bark Bark BOO!

Microsoft has been gently pushing us to change the way we use shared calendars and shared address books. They no longer recommend we use public folders for this application.

So, Scott Kjornes will be contacting all owners of Public Folder data calendars and address books and explaining different ways to accomplish the same thing.

Microsoft's suggested answer for shared calendars is for one user to create the calendar and then grant permissions to others to view only, add entries, or change entries on that calendar.

Many of you use this method already but some will be unfamiliar with this. Scott will help you do this in the coming weeks.

Have a great FALL!

Roland





Welcome to the 'New' Insider Information Format

With every part of our lives, there always comes change. Some changes are good for most, and some are only good for a few.

With the new format you see here, MIS is trying to narrow the focus of our Jefferson County network users. The change in our quarterly newsletter format, brings concise information presentation, along with the latest news in our industry that we would like to share to keep you all better informed.

Thanks for reading and remember; A mind is a terrible thing to waste. Scott K.

MIS Phone Numbers

PC/ Network		AS400 (ISIS)	
MIS Front Desk	674-5952	John Rageth	674-5954
Mike Henes	674-5965	Josh Paul	674-5955
Scott Kjornes	674-5961	Oral Rowland	674-5964
Rick Christian	674-5953	Scott Fossum	674-5957
Roland Welsch	674-5958		
Training Room	675-4800	Remember about 4 digit department dialing! FAIR, ANNEX, and PARKS Maintenance have also been added to the Cisco Corporate Phone Directory!	



Thanks to searchnetworking.techtarget.com

Experience is not what happens to you; it's what you do with what happens to you.

—Aldous Huxley

Read more at; http://www.brainyquote.com/quotes/topics/topic_wisdom.html#kmfXLOdfgScmTfBV.99



MIS Training Room

Our Courthouse Training Room is still available for training sessions as needed.

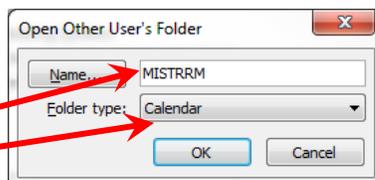
You can even reserve the Training Room and send a group of employees to the room on a quiet day, even on short notice.

Need a quiet place away from your ringing phone and busy desk to watch a **Lynda.com** video training session? You can reserve the Training Room or send a group of employees to use the room anytime.

To determine dates and times for your group and when our Training Room is available, open your **File** tab in Outlook, click **Open**, then click **Other User's Folder** utility. The Open Other User's Folder utility window will appear. Type **MISTRM**

In the **Name...** line, select **Calendar** next to Folder Type: field, then click **OK**. Calendar will appear in your Outlook Calendar.

The Training Room Calendar is available to view for all Jefferson County employees to determine when you would like to use MIS resources



NOTE: You can always get 3 or more people together and we can schedule any special classroom training session for your group.

For more information or to schedule a room reservation for your Special Training classes or use of room equipment, call Scott K. at **x5961** or Email him at scottk@jeffersoncountywi.gov

If you need AS400 training, call John Rageth at **x5954** or Oral Rowland at **x5964** to schedule a date.

LYNDA.COM and their nearly 2000 courses offered to all Jefferson County Employees



Create your Lynda.com profile from a County computer at <http://iplogin.lynda.com>, and start taking advantage of Coursework about Office 2010, Adobe, Windows, and many others offer at the click of your mouse, **24 hours a day/ 7 days a week.**