PHISHING

DON'T GET HOOKED!

Phishing email messages and websites are intended to steal your money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer. They might email you, call you on the phone, or convince you to download something off of a website.

Don't get reeled in! Look for these Phishing scam signs:

- Poor spelling and unusual grammar
- Asking you to type in your password or other confidential information for "security purposes"
- Offering a prize or reward to get you to click on a link
- Website addresses that look almost identical to the real thing but are slightly different:

  www.twiter.com vs. www.twitter.com
- Aggressive urgency to get you to respond in a panic before you even think about it
- Using masked links that look like a familiar website but take you to a different link once you click on it

  Hint: hovering over the link with your cursor will show you the real website address that the link will take you to
- Emails that appear to come from a senior employee from your company or organization

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.

mxotech

Beyond IT. People.

WHAT HAPPENS ON SOCIAL MEDIA STAYS ON GOOGLE FOREVER

Social media is a wonderful tool for staying in touch with friends and family. But remember, it isn't truly private.

Follow these tips to stay safe:

- If you wouldn't say it in person, don't say it online
- Don't put up any sensitive personal details, such as work or personal information
- Turn on your privacy settings and keep them locked so that only your most trusted friends and family can see what you post
- Log out of the application every time you're done using it (this way if you lose your phone, your accounts can't be easily accessed)
- Use a different password for all of your social media accounts

mxotech
Beyond IT. People.

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.

PASSWORDS
ARE LIKE UNDERPANTS

- **You shouldn't leave them out where people can see them**
- **You should change them regularly**
- **And you shouldn't loan them out to strangers**

Here are tips to creating a strong password:

GOOD PASSWORDS

- Are at least 14 characters in length
- Are a phrase, instead of a single word: "iLOveMYp4sswOrd!"
- Contains both upper and lower case letters and some punctuation
- Are not single words in any language, slang or dialect
- Do not include personal information such as names of family, pets, etc.

BAD PASSWORDS

- Can be found in a dictionary in any language
- Contain less than 10 characters
- Are easy to figure out like family, pets, birthdays, etc.
- Use word or number patterns

mxotech
Beyond IT. People.

Protect yourself, protect your business. MXOtech will help.

Visit www.mxotech.com/security for more information.

The 10 Disaster Planning Essentials for any business:

What you need to know to avoid losing everything in an instant

MXOtech has been named one of America's Fastest Growing Companies by Inc. 5000, one of North America's top providers of emerging technologies on the CRN Next Gen 250 list, among the country's most thriving industry leaders on the CRN Fast Growth 150 list, and one of the World's Best Managed Service Providers by MSPmentor for the last two years. CEO Joanna Sobran was honored among the Top 15 Business Women in Illinois by the Illinois Diversity Council, and included on the CRN 2018 list of best woman-owned technology companies in the nation.

Provided as an educational service by:
Joanna Sobran, President and CEO
MXOtech, Inc.
1101 West Adams Street, Suite A • Chicago, Illinois 60607
312.554.5699 • www.mxotech.com

The 10 Disaster Planning Essentials all businesses must have in place

If your data is important to your business and you cannot afford to have your operations halted for days—even weeks—due to data loss or corruption, then you need to read this report and act on the information shared. A disaster can happen at any time on any day and is likely to occur at the most inconvenient time. If you aren't already prepared, you run the risk of being caught without an effective plan to handle any disaster that may come your way. This report outlines 10 things you should have in place to make sure your business can be back up and running again in the event of a disaster.

1. **Have a written plan.** As simple as it may sound, just thinking through in ADVANCE what needs to happen if your server has a meltdown or a natural disaster wipes out your office will go a long way in getting it back fast. At a minimum, the plan should contain details on what disaster could happen, and provide a step-by-step process of what to do, who should do it and how. It also should include contact information for various providers along with username and password information for various key web sites. Writing out this plan will allow you to think about what you need to budget for backup, maintenance and disaster recovery. If you can't afford to have your network down for more than a few hours, then you need a plan that can get you back up and running within that time frame. You may, for example, want the ability to virtualize your server, allowing the office to run off of the virtualized server while the real server is repaired. If you can afford to be down for a couple of days, there are cheaper solutions. Once your plan is in writing, print a few copies and store one in a fireproof safe, one offsite (at your home) and one with your IT consultant.

2. **Hire a trusted professional to help you.** Trying to recover your data after a disaster without professional help is business suicide; one misstep during the recovery process can result in forever losing your data or weeks of downtime. Make sure you work with someone who has experience in both setting up business contingency plans (so you have a good framework from which you CAN restore your network) and experience in data recovery.

3. **Have a communications plan.** If your employees couldn't access your office, e-mail or use the phones, how should they communicate with you? Make sure your plan includes this information including MULTIPLE communications methods.

4. **Automate your backups.** If backing up your data depends on a human being doing something, it's flawed. The #1 cause of data loss is human error (people not swapping out tapes properly, someone not setting up the backup to run properly, etc.). ALWAYS automate your backups so they run like clockwork.

5. **Have an offsite backup of your data.** Always, always, always maintain a recent copy of your data off site, on a different server, or on a storage device. Onsite backups are good, but they won't help you if they get stolen, burned, hacked along with your server, or if your office is flooded.

6. **Have remote access and management of your network.** Not only will this allow you and your staff to keep working if you can't go into your office, but you'll love the convenience it offers. Plus, your IT staff or an IT consultant should be able to access your network remotely in the event of an emergency or for routine maintenance. Make sure they can.

7. Image your server. Having a copy of your data offsite is good, but keep in mind that all that information has to be RESTORED someplace to be of any use. If you don't have all the software disks and licenses, it could take days to reinstate your applications (like Microsoft Office, your database, accounting software, etc.) even though your data may be readily available. Imaging your server is similar to making an exact replica; that replica can then be directly copied to another server, saving an enormous amount of time and money in getting your network back. Best of all, you don't have to worry about losing your preferences, configurations or favorites. To find out more about this type of backup, ask your IT professional.

8. Network documentation. Network documentation is simply a blueprint of the software, data, systems and hardware you have in your company's network. Your IT manager or IT consultant should put this together for you. This will make the job of restoring your network faster, easier AND cheaper. It also speeds up the process of everyday repairs on your network since the technicians don't have to spend time figuring out where things are located and how they are configured. And finally, should disaster strike, you have documentation for insurance claims of exactly what you lost. Again, have your IT professional document this and keep a printed copy with your disaster recovery plan.

9. Maintain Your System. One of the most important ways to avoid disaster is by maintaining the security of your network. While fires, floods, theft and natural disasters are certainly a threat, you are much more likely to experience downtime and data loss due to a virus, worm or hacker attack. That's why it's critical to keep your network patched, secure and up-to-date. Additionally, monitor hardware for deterioration and software for corruption. This is another overlooked threat that can wipe you out. Make sure you replace or repair aging software or hardware to avoid this problem.

10. Test, test, test! A study conducted by Zetta found that 40% of companies test their Disaster Recovery plans once annually, but 28% admit to rarely to never testing them. If you are going to go through the trouble of setting up a plan, then at least hire an IT pro to run a test once a month to make sure your backups are working and your system is secure. After all, the worst time to test your parachute is AFTER you've jumped out of the plane.

Want help in implementing these 10 Disaster Planning Essentials? If you have at least 25 computers at your office, we'll give you a FREE Backup and Disaster Recovery Assessment ($697 value). Contact us at 312.554.5699 or at sales@mxotech.com to learn how we can get started.

Business Essentials: 7 Critical Security Measures for Mobile Computing

If you have given or plan to give your employees the ability to access company data and systems with mobile devices – DON'T... until you've read this!

Provided as an educational service by:
Joanna Sobran, President and CEO
MXOtech, Inc.
1101 West Adams Street, Suite A • Chicago, Illinois 60607
312.554.5699 • www.mxotech.com

Mobile and Cloud Computing: Benefit or Threat?

There's no doubt about it – the internet and mobile and cloud computing have made our lives easier and our businesses more productive, cost-effective and competitive. But make no mistake about it: the internet is also a breeding ground for thieves and predators, not to mention an enormous distraction and liability if not used properly. It is causing people to be casual, careless and flat-out stupid about their privacy in an increasingly litigious society where heavy fines and severe reputational damage can occur with one slipup – which is why you cannot be casual or careless about introducing it to your organization. You can't turn on the TV or read a newspaper without learning about the latest online data breach. And mobile devices are easily misplaced and stolen.

Because of all of this, if you are going to allow employees to use mobile devices – particularly personal mobile devices – to access, store and use company data, then it's critical that you have these 7 security measures in place.

1. **Implement a mobile device policy.** This is particularly important if your employees are using their own personal devices to access company email and data. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR information, or your clients' information, isn't compromised? Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can and cannot do with that device, including "rooting" or "jail-breaking" the device to circumvent security mechanisms you put in place.

2. **Require STRONG passwords and passcodes to lock mobile devices.** On a cell phone, requiring a passcode be entered will go a long way in preventing a stolen device from being compromised.

3. **Require all mobile devices be encrypted.** Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that unlocks (decrypts) the data.

4. **Implement remote wipe software for lost or stolen devices.** If you find a laptop was taken or a cell phone lost, "kill" or wipe software will allow you to disable the device and erase any and all sensitive data remotely.

5. **Backup remote devices.** If you implement Step 4, you'll need to have a backup of everything you're erasing. To that end, make sure you are backing up all MOBILE devices, including laptops, so you can quickly restore the data.

6. **Don't allow employees to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully

download malicious software by embedding it within downloadable files, games or other “innocent”-looking apps.

7. **Keep your security software up-to-date.** Thousands of new threats are created daily, so it’s critical that you’re updating your mobile device’s security settings frequently. As an employer, it’s best to remotely monitor and manage your employees’ devices to ensure they are being updated, backed up and secured.

Want help with implementing these 7 essentials?

If you are concerned about employees and the dangers inherent in mobile and cloud computing, then call us about how we can implement a mobile and cloud security and monitoring system for your business.

Our process involves documenting all the mobile devices accessing your network, documenting what cloud applications your organization uses AND determining an appropriate backup for the data stored on third-party platforms. We’ll also help you implement a mobile device policy, educate your employees on how to “stay safe” online and put critical security and backup services in place so you don’t have to worry about data loss or unauthorized access to your company’s network.

Contact us today to request a FREE, no obligation Mobile and Cloud Security Assessment!

312.554.5699 | sales@mxotech.com