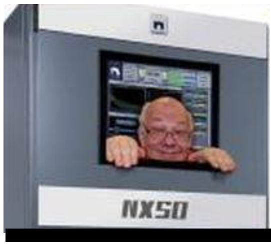


The

Broadcasters' Desktop Resource

www.theBDR.net ... *edited by Barry Mishkind – the Eclectic Engineer*

Doing IT Right

Keeping Malware at Bay

By Barry Mishkind

[September 2019] Periodically, the BDR takes note of some of the publicized hacking episodes, especially at radio stations, to alert everyone of the dangers from malware, especially ransomware, and bad actors.

Things in the IT world definitely are getting more dangerous.

In many ways, the Internet is what people used to call "the Wild West," where law and morality were not the strongest aspects of life. Around the world, attacks on servers, station LANs (Local Area Networks), and individuals are a constant danger, easily seen by inspecting server logs and email links and attachments.

To help readers, **The Broadcasters' Desktop Resource** tries to keep a continuing focus on the need to:

(1) train staff in good computer safety practices,
(2) have good, safe backups, and
(3) have a plan in case of system failure, whether due to disaster or hackers.

We invite your participation, by considering the information below, and sharing your thoughts to help others learn tactics and solutions to reduce vulnerability of station and personal computer systems and improve financial integrity.

IT TAKES ONLY A MOMENT

Perhaps the most frightening aspect of this discussion is that it merely takes a moment – one person making a single mouse click on an email link or a site compromised with malware – to completely disrupt, or even destroy, virtually everything on your computers.

So, we ask a question that is more important than ever: Do you have a plan to prevent, or recover, from such an event?

NOT JUST "A POSSIBILITY"

As this is written, the latest broadcaster to have major malware issues seems to be Entercom.

While the company sought to provide "no comment" to outsiders, reports appear to indicate an event so widespread that employees all over the country were told not even to connect laptops to the network. All corporate email was down for most of a week. And as IT specialists worked around the clock to restore services, a shadowy figure was said to demand a ransom of $500k.

While Entercom may restore their systems without paying any ransom, they are enduring costs of downtime, overtime, lost business, etc., joining several other stations and groups that have been targeted.

DANGEROUS EMAIL!

Just like the Caller ID on your phone, email addresses can easily be spoofed.

Skeptical? I am far from an IT guru, but even I know how to send you a message from virtually anyone – even yourself! – and do it in less than 30 seconds.

When you realize that more email addresses have been compromised than there are people on the planet, or when we read of some data company losing hundreds of millions of accounts, we begin to understand how big the problems have become. Too many bad actors know your name/address.

Here is how easily it can happen: if one of your correspondents gets hacked, any contact information in their "address book" may be taken. It is the primary reason when a lot of spam and malware laden emails suddenly show up.

Want to do a quick check on an email address? Try this site. After their big data loss, Experian also has a place to check to see if your personal information was grabbed in their breached data. (If so, Experian offers free reports for several years.)

Many millions of dollars have been lost and/or malware spread by someone responding to what they thought was their bosses' email, falsely directing payments or asking them to click on a link that turned out to be dangerous.

EMAIL PROTECTION

Some protection comes from one of the various anti-virus and malware programs out there that may work for you. There are several favorites.

A good IT department can be instrumental in preventing a lot of the bad stuff, though some do seem to be led by Mordoc (the Preventer of Information), and use excessively tight filters, figuring that if they block all email, nothing bad can get through. Trying to send email to such companies can be very frustrating.

But the basic lesson is not to trust any email that asks you to click on anything, unless you are sure where it came from. If someone familiar to you got hacked, email that looks like it is from them could be dangerous.

PROTECT MISSION CRITICAL GEAR

There are many other ways bad things can infect your LAN. For example, USB flash drives, CDs and DVDs from outside the building, even updates of soft-ware/firmware for studio equipment.

And then there is, not to dump too hard on them, the weekend staff.

Can you train all of these people on computer safety *and* depend upon them to act in a responsible way? Or, is the only safe answer to return to the "sneaker net" days?

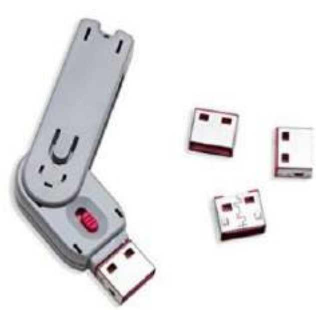
USB DRIVES

One of the biggest non-email dangers comes from USB flash drives. Why? Because they are so easy to carry – and just stick into a convenient port.

For that reason, it is almost impossible to know exactly where they have been. And any computer in which they have been inserted can potentially leave a virus behind – or worse.

And it does happen.

Perhaps one of your staffers has downloaded a new song. They bring it into the station to share and – oops – the LAN may have a time bomb planted. (Some malware essentially seeks large networks, so they do not necessarily "appear" nor attack home machines.



Many companies now disable USB ports for just this reason. Some use software. Others install little plugs or locks that require a tool or key to remove the plug.

Still others go so far as to remove, superglue something in, or otherwise damage the ports to prevent insertion.

Of course, this raises the question: What about keyboard and mouse connections to USB ports? Sometimes, just putting the CPU in a place the staff cannot reach is enough. Sometimes additional effort to prevent someone from casually pulling a cord and putting a flash drive in the slot is necessary.

OTHER DATA CARRIERS

USB flash drives are not the only way infections can pass into a computer.

CDs and DVDs, etc., coming from outside the station are also potential problems. At one time, a manufacturer of digital consoles sent out a software update – complete with a virus!

By the time it was identified (and admitted to by the manufacturer), several hundred copies of the virus were all over the console network, causing all sorts of problems.

Even file downloads can be contaminated, even from your equipment or software manufacturer. This is why it is important to ensure whatever machines are used for downloading and updating files has a strong anti-virus application on it.

Perhaps even two.

PEBCAK

You may have heard about this problem. It is among the hardest to prevent.

PEBCAK stands for "Problem Exists Between the Chair And Keyboard." Yep, it is the strange behavior of staff, especially bored weekenders. No matter what you say or how many memos you write, this is where things can go bad real fast.

Staffers do not even have to access the Internet to cause major grief. One major automation system used a hard-coded user and password, presumably to make rebooting/reloading quicker and easier. That worked fine until a weekender decided to access the system prompt and change the administrative passwords.

REDUCING PASSWORD PROBLEMS

Another major problem is when the same password is used for many apps at the station or by many people.

Sadly, "password" is still the most common one used, along with "123456" and similar variants.

Dictionary attacks try those first, which is why we keep reading how bad guys easily manage to break into many accounts.

At the same time, changes in technology have made those long "odd looking" passwords less secure than previously thought. This actually is a byproduct of all those major data breaches you read about in the news.

HOW THEY DO IT

By all means, do use a password – or better yet, a pass phrase – you can easily remember, with a number or special character added.

But consider this: after downloading data files from a breach, the bad guys just try each account with "password" or "123456" or similar guesses like that. You, too, can quickly find a list of common passwords.

Since these are so commonly used, even with systems that encrypt passwords, it does not take long for them to find an account they can attack and take over. But, worse … and here is the rub … now that they know one password, they can return to the data files and reverse engineer it to see how the encrypted passwords decrypt.

Then they can use the decryption algorithm on your encoded password and, boom, they can see yours.

Have you had an email from someone recently, with your own password in the subject line? Perhaps the text told you they now control your account. Perhaps they want a ransom not to release nasty pictures they claim to have taken with your camera.

If you have several accounts with the same password, this could be trouble. You should probably go check on your accounts and change passwords if necessary.

On the other hand, a lot of these scams are just that – scams! For example, if you are like your author, it would be very hard for them to get any video, since there is no camera on my machine!

ALL THIS POINTS TO A PLAN

If you do carefully set up, administer, and train responsible people, your system will largely be safe … until the one day that somebody does something.

IT professionals generally recommend not paying ransom – after all, crooks are not someone to trust. But sometimes it is not even a matter of ransom.

The point is: Do you have a plan … recent backups … and a way to operate should your network be compromised? Backups, especially those *not* on the same LAN are essential.

Doing the backups regularly is also important, for several reasons, including ensuring the backup software works properly.

By the way, please *do not* make and save just one backup at a time.

Why? Suppose the malware incorporates a timer, and does not become active for two weeks or more? Saving and keeping your last several backups may save you from restoring one that includes the ticking time-bomb malware.

**IS THERE
A TURNTABLE IN THE HOUSE?**

Well, maybe installing turntables is taking protection to an unreasonable point.

On the other hand, some stations actually have prepared for potential EMP (ElectroMagnetic Pulse) problems by having a working transmitter on site – but *not connected to anything.* If an EMP hit there would be a delay getting back on the air, but chances are the transmitter would work well.

A similar "fail safe" plan for program audio might include a computer loaded and set aside from the network, perhaps not even powered up (and maybe even in a Faraday Cage).

Should something happen via malware, the network can be shut down and the fail safe computer hooked to the STL chain.

Further recovery can then be achieved while something is on the air. (Pre-planned announcements should be part of the fail safe computer files.)

TIME TO REST EASY

After all is done to harden your system, protecting against malware, viruses, and other issues, is it time to be confident and relax?

Probably not. At least not entirely.

Every day, the bad guys are inventing new ways to attack, intrude, and wreak havoc. As has been mentioned on many newscasts and in newspaper reports, some countries have entire buildings full of hackers who are exploiting whatever they can find.

Some try to hit power grids, others try to extort money from hapless users. They do target hospitals, schools, and city/county government systems – any place that would grind to a halt if the computers were commandeered. Broadcasters' computer systems fit the description, do they not?

Therefore, we urge you to please keep vigilant. Read about current exploits. Train your staffers. And train them again!

We hope these tips will keep you up and running … and, yes, able to relax a bit.

- - -

Do articles like these help you get your job done? Then click here and take 30 seconds to subscribe to the One-Time-A-Week BDR Newsletter. You will learn when new articles appear.

- - -

Return to The BDR Menu