This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

RANSOMWARE AND BACKUP PLANS

Cybercrime is a Willy Wonka factory for fraud, furiously and creatively innovating both technically and psychologically. This time around, we talk about a ploy that's picked up a lot of momentum in recent years: ransomware.

Ransomwhat?

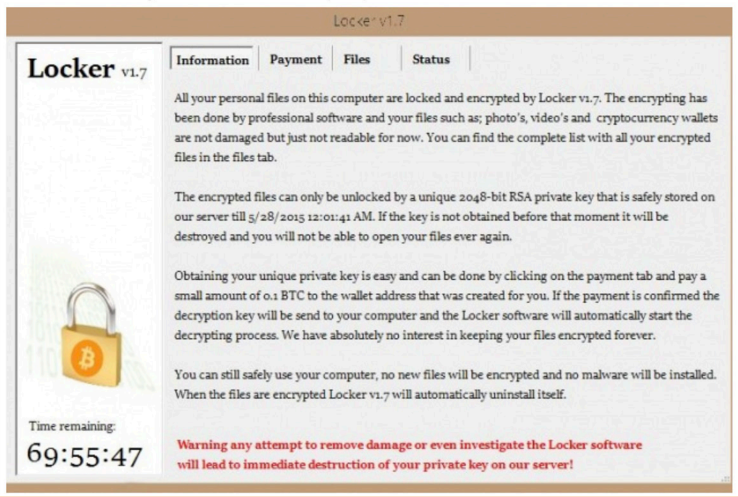
"Ransomware" is a type of malicious software designed to block access to your computer – and any connected files – until a sum of money is paid.

Just imagine – one minute you're clicking on an Excel file in a curious email and the next, you're completely locked out of your computer. Even files you've stored in "cloud" systems like Google Drive are inaccessible. Then, a scary pop-up telling you to pay up ... or else.

Even worse, these techno-kidnappers often require payment in the form of "bitcoin" which, let's face it, most of us don't even understand, let alone have easily available should we want to pay.

Ransomware attacks are causing a lot of headaches out there: downtime, data loss, intellectual property theft, data breaches ... all potential nasty side-effects of this latest hazard.

EXHIBIT A: Scary Ransomware Pop-Up



All your personal files on this computer are locked and encrypted by Locker v1.7. The encrypting has been done by professional software and your files such as; photo's, video's and cryptocurrency wallets are not damaged but just not readable for now. You can find the complete list with all your encrypted files in the files tab.

The encrypted files can only be unlocked by a unique 2048-bit RSA private key that is safely stored on our server till 5/28/2015 12:01:41 AM. If the key is not obtained before that moment it will be destroyed and you will not be able to open your files ever again.

Obtaining your unique private key is easy and can be done by clicking on the payment tab and pay a small amount of 0.1 BTC to the wallet address that was created for you. If the payment is confirmed the decryption key will be send to your computer and the Locker software will automatically start the decrypting process. We have absolutely no interest in keeping your files encrypted forever.

You can still safely use your computer, no new files will be encrypted and no malware will be installed. When the files are encrypted Locker v1.7 will automatically uninstall itself.

Time remaining:
69:55:47

Warning any attempt to remove damage or even investigate the Locker software will lead to immediate destruction of your private key on our server!

Unfortunately, it's a very successful criminal business model. After "going pro" in 2013 with the release of "CryptoLocker", there's been lots of copycat code and many new strains have continued to emerge. Hackers are making millions.

The Best Defense Is a Good … Defense

So, how do you prepare for the chance of getting hit with ransomware?

1. **Back It Up:** Ransomware works because the bad guys take control of something you greatly value – your files. But if you have backup copies of important files, these cryptocreeps lose their leverage. Start backing up your files today. And don't stop (see below for more on creating back-ups).
2. **Don't Fall for It:** Remember the safety rules!
   - Don't open unsolicited attachments or links.
   - When in doubt, contact the sender separately to verify they intentionally emailed you that document, link, or request.

Backups Got Your Back

Right. Back-ups. How do those work, again?

WHAT TO SAVE: Anything you'd shed tears over if it disappeared for good (e.g. that spreadsheet you've been perfecting for the last three years). So if you got hit with ransomware, you could readily recover this stuff on your own, ransom-free.

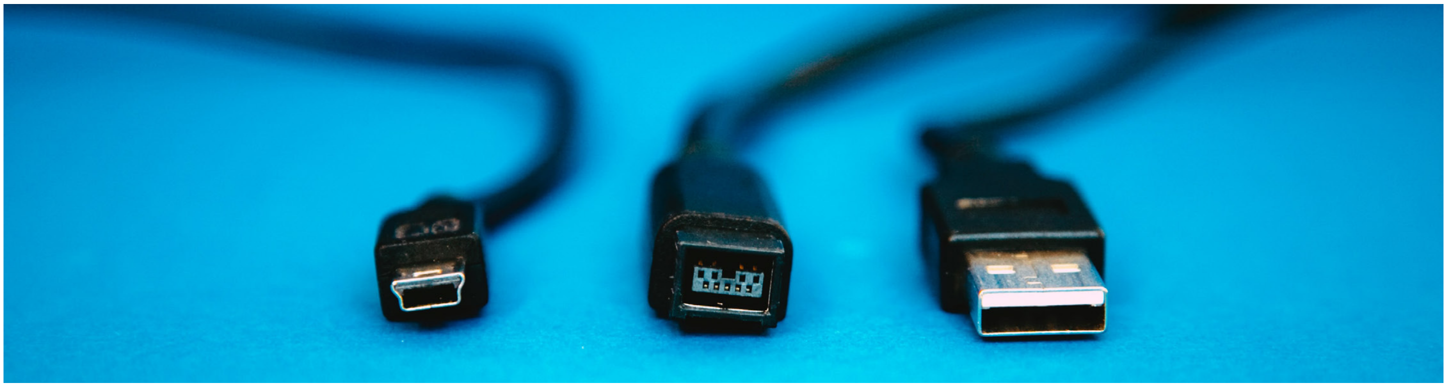
WHEN TO SAVE: Depends on you. If it's something really important that changes frequently, back it up more frequently. If it's something more static (like family pictures), maybe back up a batch every 3-6 months. Like insurance, it comes down to your personal tolerance for risk.

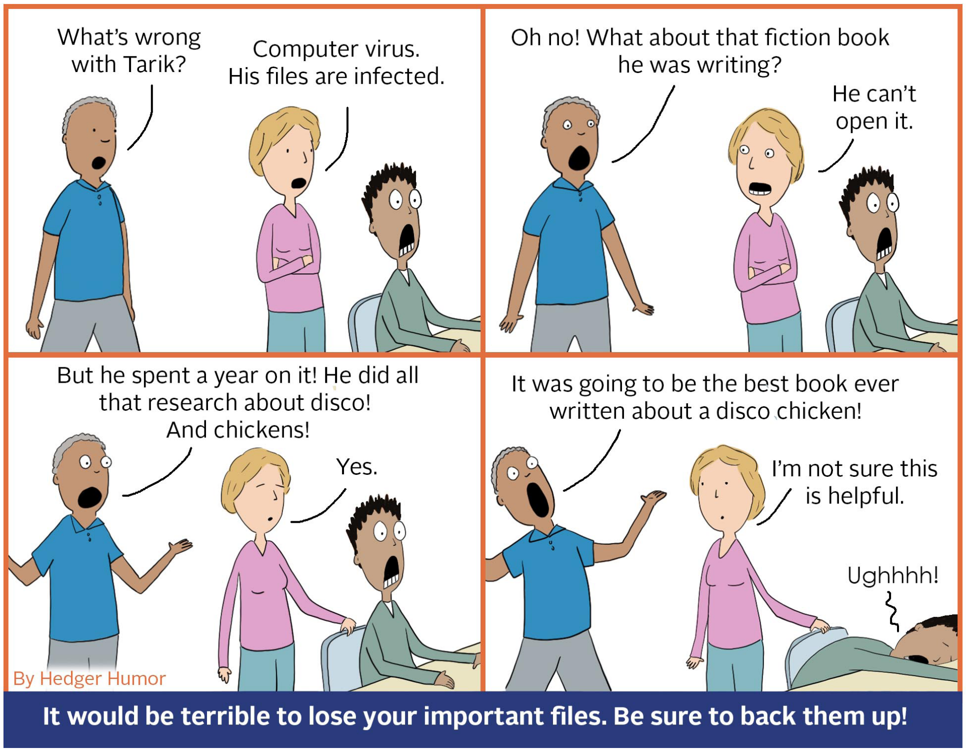
WHERE TO SAVE: Storing stuff in the cloud is usually fine, but for threats like ransomware, a good ole' fashioned "ground" copy is best. Consider investing in an external hard drive (for long-term storage) or encrypted USB drive (for shorter-term, lower volume storage). And it's a good idea to "air gap" that drive (disconnect it physically from your computer) since ransomware that hits your machine will go looking for connected drives.

A word about "standard" USB drives

These little fellas sure are convenient, but they're easily lost. So no sensitive or private data on a USB drive unless it's the "encrypted" variety, please.

And another word about "standard" USB drives – did you know some hackers are loading malicious code on these drives and leaving them around public places, tempting a passerby to pick it up and plug it in somewhere? (Yup. Here's A Few Words about Found USB Devices for you.) So remember what your mother taught you: If you don't know where that thing's been …




What's wrong with Tarik?
Computer virus. His files are infected.
Oh no! What about that fiction book he was writing?
He can't open it.
But he spent a year on it! He did all that research about disco! And chickens!
Yes.
It was going to be the best book ever written about a disco chicken!
I'm not sure this is helpful.
Ughhhh!
By Hedger Humor

It would be terrible to lose your important files. Be sure to back them up!

Learn more about Becoming Cybermindful at go.udayton.edu/cybersecurity

Scam Self-Defense: Would You Know if Your Email Was Hacked?

By now, you're probably getting pretty good at scenting the signs of a phishy email. But, if one stinky click landed you in a scammer's phish-bowl, how would you know?

Telltale Signs Your Email Has Been Hacked:

- Suspicious sign-in email alerts in your inbox or trash
- Messages marked as read that you didn't read
- Sent items you didn't send
- Delivery failure notification messages

If you see a sign (and are we the only ones who hear that 90's Ace of Base song in our heads when we read that?), change your password immediately and keep an eye on your other online accounts for potential cross-compromise (Pro Tip: watch A Few Words about Knowing if Your Email Address is Compromised.) If you think you might have clicked (it happens!), contact your organization's IT support team.

Speaking of signs, it's well past time we sign off and let you get back to your day. See you next time, cybermindful compatriots!

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for
Cybersecurity &
Data Intelligence

OHIO CYBER
RANGE INSTITUTE