

Your Personal Cyber Security Checklist

1. Global Cyber Crimewave Accelerants

- _____
- _____
- _____
- _____

2. Old School Prevention

- Keep a primary checking account where all outbound flows are controlled by you
- Have a secondary checking account for occasional physical checks and any “pull” transactions, especially from payment solutions like Venmo and Paypal
- Use the bank’s app and setup notifications for any unusual transactions
- Use an identity monitoring AND recovery service
 - Get one that will assist you in the recovery, like ID Shield
- Lock/Freeze your credit whenever you are not opening new credit accounts

3. Practice Good Cyber Hygiene

- Apply updates as soon as they are available
- Purchase a good firewall/wifi router that is kept up to date and don’t use the default passwords
- Use a good antivirus software, even if you have a Mac
 - Webroot
 - Sophos
 - TrendMicro
 - See av-test.org for more reviews
- Don’t install apps or plugins just because you are prompted to do so
- Use an ad-blocking program like Ad Block Plus (<https://adblockplus.org/>)
- Disable unused browser extensions and add-ins (like coupon applications)
- Backup your data offsite (aka “air-gapped” backup)

4. Be Aware!

- Be suspicious of every e-mail
- Verify ANY financial info via a secure, secondary communication channel
- Hover over links to verify source – don’t click them if you are unsure!
 - Open websites directly, rather than by following links in email
- Don’t publish your e-mail address anywhere on the Internet (verify with Google search)
- Subscribe to breach monitoring (<https://haveibeenpwned.com/>)
- Look for https: when inputting any data

5. Password Management

- Set a different password for every account and website**
- Don’t share your ID and password with anyone**
- Use randomly generated complex passwords or passphrases**
- Use a password manager like Lastpass
- Use multi-factor authentication (MFA) wherever possible

Your Company Cyber Security Checklist

1. Old School Prevention

- Setup controls and limits on ACH and wire-transfers
- Use check positive pay, or use a separate account to write checks out of
- Call your insurance broker and make sure your cyber coverage is adequate.
 - If your broker isn't familiar with cyber risks, find one who is
- Have an incident response plan that includes your insurance provider and legal counsel

2. Manage and Protect Company Endpoints

- Centrally manage and monitor all of your systems to ensure they are updated, encrypted, and protected
- Endpoint protection software should prevent malicious software from executing, detect unusual activity, remediate damage, and provide forensic information. It should feature behavior-based AI-enabled threat detection, not just signature-based detection
- Test your protection at <https://www.knowbe4.com/ransomware-simulator>

3. Harden Your Perimeter and Monitor Your Interior

- Protect your network with a current generation firewall that properly controls traffic into AND out of your network
- Monitor and log for suspicious activity on your network and endpoints
- Implement a Security Information and Event Management System (SIEM)
- If you already have a SIEM, add Detection and Response (XDR) capabilities

4. Educate and Test Your Employees

- Provide ongoing security awareness training and information
- Phish-test your employees at least monthly

5. Control Your Company's Password risks

- Provide a password manager for all employees that need to access multiple online services for their job
- Implement a single sign-on (SSO) system to minimize passwords
- Enforce Multi-Factor Authentication (MFA)

Presenter Info:

Tim Rettig

President & CEO

Intrust IT

www.intrust-it.com

(513) 842-3160

www.linkedin.com/in/timrettig

Additional Resources

1. <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
2. <https://www.guern.net/Black-market%20survival>
3. <http://www.databreachtoday.com/>
4. <https://krebsonsecurity.com/>
5. <http://www.clarkhoward.com/>
6. <https://www.torproject.org/>
7. <https://bitcoin.org/>
8. *Deep Web the Movie* <http://www.deepwebthemovie.com/>
9. Documentary: *The Rise and Rise of Bitcoin* <http://bitcoindoc.com/>
10. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It*
by Marc Goodman
11. *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door* by Brian Krebs
12. *American Kingpin: The Epic Hunt for the Criminal Mastermind Behind the Silk Road* by Nick Bilton