



# Data Privacy Detective Podcast – Episode 4 – Your Personal Checklist for CyberSecurity

---

Oct 17, 2016

**Categories:**

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

**Authors:**

[Joseph J. Dehner](#)

After lunch at a conference, the mental gap between speaker and listener can widen. Minds drift. Our cell-phones and smartphones tempt us to turn our attention from the speaker to the devices to which we've become addicted.

On a Chicago fall afternoon in 2016, John Hibbs, Chief Information Security Officer for J.P. Morgan Chase gave a riveting talk about the very devices that tempt us to spend our waking hours giving them attention. He spoke about the choices we make to expose our personal data to unwanted exposure. He began with a challenge I readily accepted – that humans are not good at guarding our data privacy. Technology is too strong and changing too quickly to keep up with it. Nonetheless, there are choices we can make in choosing the equipment and software we use and so increase our data privacy. We are our first line of defense against the loss of our privacy.

So make notes of this checklist and become a worthy guardian of your own, your family's and your company's data.

First, email. First-rate email providers envelope your information with multiple layers of security. Ask your email provider if it offers these features, and if not, move to one that does:

- Secure authentication to prevent spam and spoofing
- Virus scanning
- A strong spam filter
- Phishing protection (which is less common than other features just mentioned).

Get and use different email addresses for different purposes. Don't mix personal and business email addresses.

Second, passwords. We fear forgetting our passwords, so we use repeat and weak passwords, making it easy for hackers to access

our accounts. A good password manager can create high-level protection. Available for an annual cost of under \$40, password managers can give you secure and private access from anywhere across your devices and generate for you complex passwords while giving you a single, encrypted entryway to access your sites that require a password. This eliminates memory loss and greatly heightens the security of your most sensitive information. The manager never knows your actual identity, so is unable itself to be hacked to reveal it.

Third, virus and malware protection. Anyone using a computer to web surf, shop, bank, email or instant message without proper protection is at high risk of becoming a victim of identity theft and financial loss. Real-time running of anti-virus protection reduces infection risk by about 80%. Some providers offer backup protection as well, so that data is protected from system failure.

Fourth, your wireless router, at home or work. Routers let several devices access the internet and interact. Routers are themselves computers, and so are subject to hacking and other risks. If a hacker gains access to your router, your entire set of accounts on devices is at risk. Replace your router every two years, and buy one that has Distributed Denial of Service Protection, a good firewall and a separate guest network and temporary access for guests if you let them use your router.

Put these tips to use and you'll increase the privacy of your personal data. Technology will not make these choices for you. Remember, protecting your personal data starts with you.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law Industry Group](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.