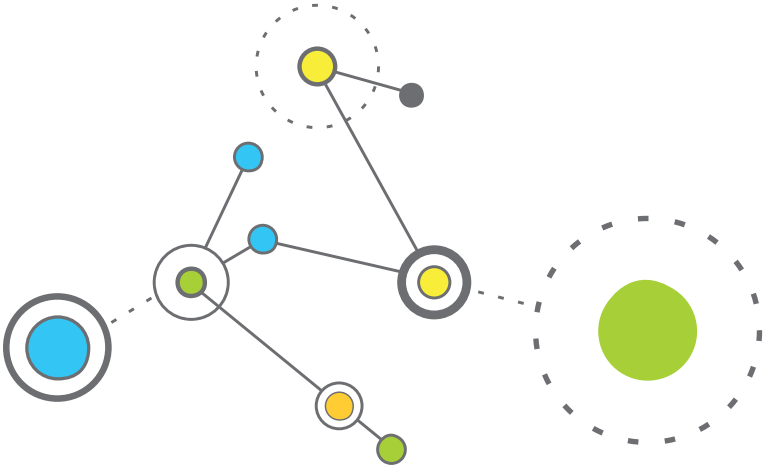
CAREFUL CONNECTIONS

Building Security in the Internet of Things



Federal Trade Commission | business.ftc.gov

It's called the Internet of Things – the burgeoning phenomenon of day-to-day consumer products and services that connect to the Internet. Maybe it's a simple convenience like a home automation system that turns lights on and off remotely. Other innovations have the potential to save lives – for example, a connected car that contacts first responders instantly in case of an accident or a mobile app that allows a patient to share vital signs with a doctor. What distinguishes the Internet of Things is the product's ability to use the Internet to communicate with us, with others, or with other devices.

The Internet of Things has the potential to offer enormous benefits to consumers. Innovative companies are already selling connected devices, apps, sensors, services, etc., unlike anything we've seen before. But businesses need to consider security, too. As with any online activity, it's important to protect consumers' sensitive data from thieves. The Internet of Things, however, adds new security dimensions to consider. For example, an insecure connection could give a hacker access not just to the confidential information transmitted by the device, but to everything else on a user's network. And in the Internet of Things, the risk isn't just to data. If that home automation system isn't secure, a criminal could override the settings to unlock the doors. And just think of the consequences if a hacker were able to remotely recalibrate a medical device – say, an insulin pump or a heart monitor.

Businesses and law enforcers have a shared interest in ensuring that consumers' expectations about the security of these new products are met. Like any other industry in its infancy, the Internet of Things must prove itself worthy of consumer confidence. Is your company taking reasonable steps to protect consumers' devices from hackers, snoops, and thieves?

There's no one-size-fits-all checklist to guarantee the security of connected devices. What's reasonable will depend on a number of variables, including the kind and amount of information that's collected, the type of functionality involved, and the potential security risks. But based on input from industry, consumers, academics, and others, the FTC has a series of steps for your company to consider if you're designing and marketing products that will be connected to the Internet of Things.

Start with the fundamentals.

When it comes to security, the technology is ever-changing, but certain time-tested tenets have emerged.

- Encourage a **culture of security** at your company. Designate a senior executive who will be responsible for product security. Train your staff to recognize vulnerabilities and reward them when they speak up. If you work with service providers, clearly articulate in your contracts the high standards you demand from them.
- Implement **"security by design."** Rather than grafting security on as an afterthought, build it into your products or services at the outset of your planning process.
- Implement a **defense-in-depth approach** that incorporates security measures at several levels. Walk through how consumers will use your product or service in a day-to-day setting to identify potential risks and possible security soft spots.
- Take a **risk-based approach**. Unsure how to allocate your security resources? One effective method is to marshal them where the risk to sensitive information is the greatest. For example, if your device collects

and transmits data, an important component of a risk-based approach is an up-to-date inventory of the kinds of information in your possession. An evolving inventory serves triple duty: It offers a baseline as your staff and product line change over time. It can come in handy for regulatory compliance. And it can help you allocate your data security resources to where they're needed most. Free frameworks are available from groups like the Computer Security Resource Center of the National Institute of Standards and Technology, or you may want to seek expert guidance.

- Carefully **consider the risks** presented by the collection and retention of consumer information. If it's necessary for the functioning of your product or service, it's understandable that you'd collect data from consumers. But be sure to take reasonable steps to secure that information both when it's transmitted and when it's stored. However, it's unwise to collect or retain sensitive consumer data "just because." Think of it another way: If you don't collect data in the first place, you don't have to go to the effort of securing it.
- **Default passwords** quickly become widely known. Don't use them unless you require consumers to change the default during set-up.

Take advantage of what experts have already learned about security.

The product may be brand new, but you're not writing on a blank slate. There's a lot you can pick up from the 20 years of lessons learned by security experts. They've already identified solutions to some common concerns raised by the Internet of Things. Another excellent source of guidance is industry best practices. Here are a few

back-to-basics suggestions that have become standard operating procedure for security-conscious companies.

- Standard **encryption techniques** are available for data your device transmits and for what it stores. Select stronger encryption methods over weaker ones (e.g., you can do better than WEP).
- Add **"salt"** – random data – to hashed data to make it harder for attackers to compromise.
- Consider using **rate limiting** – a system for controlling the traffic sent or received by a network – to reduce the risk of automated attacks. Some scammers try to break into networks by using software that enters possible passwords over and over again until they hit pay dirt. Rate limiting can help thwart that kind of attack.

Design your product with authentication in mind.

Authentication – assuring that people are who they say they are – has always been important online. Proper authentication also is a must in the Internet of Things. If a device transmits or receives sensitive data, an authentication failure could allow unauthorized access to that information. But with connected devices, the risk doesn't stop there. An authentication failure could expose sensitive data not just on the device, but on networks to which it's connected. In addition, if an unauthorized person is able to access a device remotely and change how it operates, the safety implications could be profound. Consider investing additional resources in the design, implementation, and testing of authentication. If the risks are substantial, is it appropriate to put two-factor authentication in place – for example, requiring the use of a password and a secure token?

Protect the interfaces between your product and other devices or services.

Just as burglars look for unlocked doors, hackers case networks for security soft spots. Even the strongest dead bolt offers no security if the windows are left open. Of course, you've considered all the ways consumers will access your products, but have you thought about whether those entry points might be misused by attackers? A security weakness at the point where a service communicates with your device could give scammers a foothold into your network. That's why each of those interfaces needs to be secured. One example is the interface between a mobile device and the cloud. Here are two particular web-based threats to guard against: cross-site scripting (XSS) attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery (CSRF) attacks, where unauthorized commands are sent from a user the website trusts. Fuzzing – a testing method that sends a device or system unexpected input data to detect possible defects – is a good approach. Consider using manual and automated tools to test interfaces. A simple online search will yield some helpful ones. Just be sure they're from groups you know to be trustworthy.

Consider how to limit permissions.

When consumers use your product, chances are you'll need access to certain data to make it work as advertised. But given the risk if an interface is compromised, it's wise to be wary of accessing information you don't really need. Experts call it the principle of least privilege – crafting permissions to limit access to the level that will allow for normal functioning. Savvy businesses take time to think through the implications of those choices to strike the balance in a way that promotes utility and security.

Take advantage of readily available security tools.

There's a tool out there for most basic security testing tasks – network scanning for open ports, reverse engineering of programming code or decompiling, checking password strength, and even scanning for known vulnerabilities. Many of these tools are free, and some of them work automatically. Of course, using them can't guarantee security, but they're important – and cost-effective – parts of a comprehensive program.

Test the security measures before launching your product.

Of course, you're eager to get to market, but make sure your product is ready for prime time. And don't just evaluate the in-the-box item. Try it out in scenarios that replicate how consumers will use the product in the real world – for example, with optional features. Are your security precautions working in those foreseeable situations? Have you closed back doors through which hackers could access information or gain control of the device? If you've turned security measures off during testing, be sure to switch them back on before going live.

Select the secure choice as your default setting.

Choose safer options as your default settings. That offers out-of-the box protection for users new to the technology, but gives experts the alternative to make the selections that best suit their needs.

Use your initial communications with customers to educate them about the safest use of your product.

Developers aim for a plug-and-play experience for buyers. That's great, but take advantage of just-in-time opportunities to educate consumers about making sensible security choices. For example, the initial registration email you send to new customers offers a timely opportunity to showcase your security features and explain how customers can use them most effectively.

Establish an effective approach for updating your security procedures.

If you're going to play in the Internet of Things arena, security can't be a one-and-done proposition. Your company may already conduct security evaluations every so often. That's an important step, but also re-evaluate your security practices as the environment changes – for example, when you deploy new technology, bring on additional service providers, or introduce new products. Other key considerations:

- How will you provide **updates for products** that are already out there? Will you offer them for free? Will updates happen automatically? It's wise to implement a belt-and-suspenders approach to reach as many of your users as possible. For example, if you need to get important security information to consumers, send a message to everyone who registered their product, contact people who signed up for news and updates, *and* put a prominent notice on your website. Some companies use on-the-product alerts – say, a small LED light – that cues users to visit the website for more information.

- Even if your company has moved on to the Next Big Thing, consider your obligations to customers who bought **earlier versions** of your product. How long will you offer security updates and patches?
- If the nature of the product makes updates unfeasible, consider how you'll respond if a significant **security flaw** is identified. How will you contact people to tell them about the problem? Product registration is one solution, but let's face it: Some consumers don't register products out of privacy considerations or concerns that information will be used for marketing. Forward-thinking companies prominently explain up front to consumers why it may be important to contact them in the future with critical security information.

Keep your ear to the ground.

Security is a dynamic process, and one advantage is the cross-talk that goes on among tech experts, researchers, and your customers. Some recent law enforcement actions have cited companies' failure to follow up when credible sources warned them about security vulnerabilities in their products. That's why it's wise to take advantage of the wealth of expertise that's already out there and listen to what people are saying about your products and the technologies you use. What else can you do?

- Stay on top of the latest threats by signing up for **email updates or RSS feeds** from trusted security sources.
- Mark your calendar to check **free databases of vulnerabilities** identified by vendors and security researchers regularly – for example, the National Vulnerability Database. In particular, check for vulnerabilities in third-party components that are integrated into your products.

- Maintain **a channel where security researchers or consumers can reach you** about a risk they've discovered in one of your products. Rather than relying on a routine "contact us" link that sends an automated reply, consider a hotline approach like an easy-to-find email box on your website that you monitor regularly. Serious inquiries related to the security of your products should generate serious responses.
- One method some companies have adopted: **bug bounty programs** that offer rewards – perhaps free products or cash – to people who identify significant security vulnerabilities in their products.

Innovate how you communicate.

You're ready to introduce a first-of-its-kind product. Don't hamper your chance for success by talking to consumers like it's 1999. Experienced marketers know that when you're explaining security or privacy options, dense blocks of fine print, complicated legal or technical jargon, and hard-to-find hyperlinks don't communicate information effectively. What's more, the next generation of products may not even have a screen. Now is the time for companies to put their creative talents to work to meet the communications challenges posed by the Internet of Things. Here are some methods to consider:

- Use a **set-up wizard** to walk consumers through the process of implementing security features.
- Build in a **dashboard** or profile management portal to make it easier for consumers to find the security settings for your device, configure them, and change them later.

- Let consumers set up **"out of band" communication channels.** For example, design your device so people can choose to get important information via email or texts.
- Use icons, lights, or other methods to **signal** when an update is available or when the device is connected to the Internet.

Let prospective customers know what you're doing to secure consumer information.

Right now, many companies still think of security as primarily defensive – behind-the-scenes precautions to help prevent the what-ifs. But the Internet of Things offers entrepreneurs an opportunity to showcase the steps they're taking to keep information safe. The likely winners in the burgeoning Internet of Things marketplace are companies that out-innovate the competition both on the effectiveness ***and*** security of their products.

ONE FINAL NOTE

Of course, it's important to keep tabs on the latest developments in security, but developers also should consider how long-standing consumer protection principles apply to the Internet of Things. When making objective claims about your product, do you have appropriate proof to support what you say? Are your billing practices transparent? Are you honoring the promises you've made to consumers about their privacy? The FTC has free compliance resources at **business.ftc.gov**.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, How to File a Complaint, at www.ftc.gov/video to learn more.

The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Federal Trade Commission
business.ftc.gov
January 2015