

Free FTC Materials For Small Business

For years, the FTC has provided education and outreach to help businesses improve their cybersecurity. Currently, the FTC offers cybersecurity guidance to businesses through written publications, websites, videos, webinars, and presentations. We partner with industry associations, trade groups, and other government agencies to help disseminate this guidance widely.

A. Written Publications

The FTC distributed nearly 400,000 cybersecurity publications in print for businesses in 2017. These publications educate and explain key elements of cybersecurity, offer practical tips for safeguarding personal and sensitive information, and outline what businesses should do if they experience a data security breach. The FTC's core cybersecurity publications include *Start with Security: A Guide for Business*,³ *Data Breach Response: A Guide for Business*,⁴ *Protecting Personal Information: A Guide for Business*,⁵ and the *Stick with Security*⁶ blog series.

Start with Security is a great place for any business to begin to learn more about the FTC's cybersecurity business guidance. It distills from the FTC's data security cases ten lessons for businesses of all sizes, in all sectors. The lessons help businesses understand security best practices – such as having strong passwords, storing information securely, and keeping security up to date. Industry associations, banks, law firms, tax practitioners, churches, police departments, nonprofit organizations, and thousands of other organizations have ordered this free publication from the FTC. In fact, the FTC has distributed more than 150,000 printed copies since first releasing this publication in 2015. In fiscal year 2017, alone, the FTC distributed almost 60,000 copies in English, plus an additional 10,000 in Spanish.

Many organizations include the lessons from *Start with Security* in their own cybersecurity presentations. For example, the National Cybersecurity Alliance (NCSA) incorporated *Start with Security* in its CyberSecure My Business workshops, which attract hundreds of small business owners every month. Also, the Virginia Governor's office co-branded *Start with Security* and made it available to businesses in Virginia. *Start with Security* had more than 6,400 views on the FTC website in the last six months. Other organizations link to it or have it posted on their own

³ Available at www.FTC.gov/StartWithSecurity

⁴ Available at <https://www.ftc.gov/tipsadvice/businesscenter/guidance/databreachresponseguidebusiness>

⁵ Available at <https://www.ftc.gov/tipsadvice/businesscenter/guidance/protectingpersonalinformationguidebusiness>

⁶ Available at <https://www.ftc.gov/tipsadvice/businesscenter/guidance/sticksecuritybusinessblog-series>

⁷ www.FTC.gov/Bulkorder

sites. For example, both the Small Business Subcommittee of the U.S. House of Representatives and the Small Business Administration (SBA) posted the publication on their websites.

Data Breach Response: A Guide for Business is another important publication. It provides practical steps for businesses in the event of a data breach. It includes, for example, a model breach notification letter that businesses can use to notify victims affected by a breach. It also offers tips on fixing vulnerabilities and securing operations after a breach. The FTC first released the guide in 2016 and since then large and small organizations have ordered more than 100,000 copies. These organizations include accounting firms, small law firms, community banks, credit unions, nonprofit organizations, local retailers, and libraries, along with state attorneys general, other local and federal government agencies, and large utility companies. The online version had more than 11,400 views in the last six months.

While the *Data Breach Response* publication gives businesses tools they need to react to a breach, another FTC publication, *Protecting Personal Information: A Guide for Business*, helps businesses be proactive. It provides practical tips for creating and implementing a plan to protect customers' personal information, and advice on preventing breaches and unauthorized access in the first place. The FTC distributed nearly 97,000 copies of this publication in fiscal year 2017. The FTC first released this publication in 2007 and has updated it regularly to reflect advice on the latest trends. Online, this publication had more than 14,000 views in the last six months of 2017.

The FTC also addresses privacy and data security topics on its business blog, which has more than 65,000 subscribers. Some of the topics covered by the business blog include how the National Privacy Policy (NPP) will affect small businesses, how to create a privacy policy, and how to handle data breaches. The FTC also provides guidance on how to create a privacy policy, how to handle data breaches, and how to create a privacy policy.

theft victims can use the site to create a personal recovery plan, file letters and forms to send to credit bureaus and businesses, and create an account to track progress and update their recovery plans. More than 600,000 people have created individual accounts since the site launched in January 2016.

C. Videos

The FTC has created a series of helpful videos to provide security tips to businesses. These videos help businesses learn how to keep their networks secure and train employees to recognize cybersecurity threats. For example, each of the ten lessons in the *Start with Security Series* includes a short video on issues like access controls, encryption, monitoring service providers, e6(air)54 -2 (i).

small businesses nationwide. In 2016, the SBA hosted a series of webinars with the FTC and

business. FTC staff also presented at their annual conference in 2016 and in 2017. The BBB another regular partner *Trusted* magazine featured an article on *Start with Security* in 2016, and the BBB often invites FTC staff to present at their local events.

Through collaboration with these organizations, we have been able to disseminate our advice to a much wider range of businesses than we could ever have reached alone.

New Small Business Initiative

Building on this strong foundation, during 2017, the FTC focused its cybersecurity education and outreach efforts to the needs of small businesses. To achieve this goal, we launched a new website and hosted a series of roundtables across the country.

A. New Website: [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness)

In the spring of 2017, Acting Chairman Ohlhausen directed the agency to create [FTC.gov/SmallBusiness](https://www.ftc.gov/SmallBusiness), a new website that helps small businesses and nonprofit organizations avoid scams, protect their computers and networks, and keep customers' and employees' data safe. The website includes written guidance, as well as videos that show businesses how to secure data in their care.

One recent example of information that small businesses can find on this site is our [article](#),

The roundtable discussions took place in Oregon, Iowa, Ohio, Delaware, and North Carolina. There were 105 owners and employees of businesses and profit organizations at each of the five roundtable discussions. They represented very small organizations, with fewer than 10 employees. Participants included a business management consultant, commercial space realtor, insurance agency owner, cleaning company owner, copy and printing services business owners, gas station consultant, accountant, executive coach, graphic designer, attorney, bookkeeper for a nonprofit organization, and other solo practitioners. These businesses reported they generally do not have full-time information technology staff to help them keep up with the latest trends in cybersecurity.

We asked the participants to share their main concerns regarding their business' cybersecurity efforts and their biggest challenges when it comes to protecting personal information. We also wanted to know where they currently get cybersecurity information and how they believe the government can help.

What we heard:

- Small business owners reported being concerned with cyber threats, but said they were overwhelmed by how to address perceived threats.
- Most people said they were concerned about human error — their own employees or themselves doing something that inadvertently would compromise the business' systems.
- Phishing schemes, ransomware attacks, tech support scams, and imposter scams were near the top of their cybersecurity concerns. Participants also mentioned mobile device security, cloud security, wireless connections, how to use email authentication, and what to look for when purchasing web hosting services.
- Many people mentioned that they were aware of the NIST cybersecurity framework, but that they needed simpler information to understand it and to learn how to implement it in their business.
- Business owners reported that they would like to better understand cyber insurance

o 2 (t)-2 (p[(he)-6 (y)20 (ne)-6 (e(s)-1 (s)-13 (or)3 J 0 m04 Tw0r)3 (m)os)15 (ec20d)-2 (e)4 (o

Plans for a 2018 Small Business Cybersecurity Education Campaign

Based on the lessons learned in the roundtable, the FTC staff will develop and implement a national cybersecurity education campaign for small businesses that will launch in 2018. The campaign will take advantage of existing resources, including staff in the FTC's Division of Consumer and Business Education and the Division of Privacy and Identity Protection. We will invite key federal agencies to participate, as well as additional partners to help extend the campaign's reach.

A. Create a suite

B. Develop consistent messages from the federal government

Small business owners and managers asked for a unified message from the federal government. Through the Cybersecurity Forum for Independent and Executive Branch Regulators ("Cybersecurity Forum"), the NCSA's federal partners working group, and other working groups