Engage, Connect, Protect

The FTC's Projects and Plans to Foster Small Business Cybersecurity

STAFF PERSPECTIVE | APRIL 2018

Cybersecurity is a critically important topic for small businesses in the United States. In a series of discussions with Federal Trade Commission (FTC) staff and partners in 2017, many small business owners said they would benefit from learning more about inexpensive, clear, easy-to-use resources about cyber threats and how to deal with them. This report describes the FTC's plain-language materials for small businesses and non-profit organizations that generally do not have in-house information technology staff. It explains the FTC's partnerships with federal agencies and industry associations to promote cybersecurity in small organizations. It also details the FTC's plans to commence in 2018, in partnership with other key federal agencies, a campaign to educate small businesses on cybersecurity.

Background

Small businesses make up a large and vital segment of the U.S. economy. They are critical to our nation's economic strength, to building America's future, and to helping the U. S. compete in today's global marketplace. There are nearly 30 million small businesses[1] in the U.S., including nearly four million microbusinesses — businesses with fewer than ten employees.[2] As engines of the U.S. economy, these small businesses employ millions of Americans and spend billions of dollars on goods and services.

Unfortunately, cyber attacks on small businesses threaten their reputations, their profit margins, and in some cases, even their survival. At the direction of Acting Chairman Maureen Ohlhausen, the FTC focused its recent business outreach efforts on helping small businesses protect their computers and networks, keeping their customers' data safe, avoiding scams — and protecting their bottom line. This report discusses the FTC's current cybersecurity business education, our recent small business cyber initiative, and our plans for future small business cyber education.

[1] https://www.sba.gov/sites/default/files/508FINALAug17Microbusiness.pdf

[2] https://www.sba.gov/sites/default/files/508FINALAug17Microbusiness.pdf

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 are free 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, non-profit organizations, and thousands of other organizations have ordered this free publication from the FTC.[7] 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/tips-advice/business-center/guidance/data-breach-response-guide-business

[5] Available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business .

[6] Available at https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-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, non-profit 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 Institute for Standards and Technology (NIST) cybersecurity framework relates to the FTC's long-standing approach to data security[8]; how to protect consumer privacy in connected rental cars[9]; and how to comply with the Children's Online Privacy Protection Act (COPPA).[10]

Last year, the FTC launched *Stick with Security*,[11] a series of FTC business blog posts that build on the *Start with Security* principles, drawing from the lessons of recent law enforcement actions, closed investigations, and experiences companies have shared with the FTC. Each blog post uses hypotheticals to take a deeper dive into steps companies can take to safeguard sensitive data. Universities, IT specialists, law firms, technology associations, and many others with thousands of followers have promoted *Stick with Security* on their social media channels. Newsfeed

---

[8] Available at https://www.ftc.gov/news-events/blogs/business-blog/2017/03/new-video-nist-cybersecurity-framework-ftc

[9] Available at https://www.ftc.gov/news-events/blogs/business-blog/2016/08/leaving-info-behind-rental-cars

[10] Available at https://www.ftc.gov/news-events/blogs/business-blog/2018/01/vtech-settlement-cautions-companies-keep-coppa-covered-data

[11] Available at https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series

websites such as Bloomberg BNA and Lexology have picked up the blog series, as well as the National Law Review, among other business resources.

In addition to general guidance about cybersecurity, the FTC has publications that address specific threats as well as the needs of particular industries. For example, the FTC has issued blog posts describing how to defend against ransomware,[12] what to do about compromised business email accounts,[13] and how to use email authentication to prevent phishing.[14] The FTC also has developed tips about ways to provide security for connected devices in our publication, *Careful Connections: Building Security in the Internet of Things*.[15] Recently, the FTC's Office of Technology Research and Investigation issued *Do Web Hosts Protect Their Small Business Customers with Secure Hosting and Anti-Phishing Technologies?*[16], which examined the security features offered by certain web hosting services that cater to small businesses.

B. Websites

The FTC's Business Center[17] is a central repository for all of the agency's online business guidance on a wide range of topics, including the privacy and data security publications discussed above. In addition to the Business Center, the FTC created two specific websites that help businesses protect their customers' personal information:

- A website for developers of health-related mobile apps,[18] which includes a web-based tool designed to help businesses understand what federal laws and regulations might apply to them. The FTC developed this tool in conjunction with the Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA).
- The enhanced IdentityTheft.gov (RobodeIdentidad.gov in Spanish), a free, one-stop resource people can use to report and recover from identity theft. The FTC encourages businesses to refer identity theft and data breach victims to IdentityTheft.gov. Identity

[12] Available at https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look

[13] Available at https://www.ftc.gov/news-events/blogs/business-blog/2017/03/has-phishing-scam-hooked-your-companys-good-name

[14] Available at https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication

[15] Available at https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

[16] Available at https://www.ftc.gov/reports/do-web-hosts-protect-their-small-business-customers-secure-hosting-anti-phishing

[17] Available at https://www.ftc.gov/tips-advice/business-center

[18] Available at https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

theft victims can use the site to create a personal recovery plan, get pre-filled 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, and building security into the development of new products. The videos are available online at FTC.gov/StartWithSecurity and on their own playlist on the FTC YouTube channel at YouTube.com/FTCvideos.

The FTC also has created videos on ransomware[19] and compromised business email.[20] These videos distill complex messages into plain-language explanations of what these threats are and how to prevent and respond to them. A third video talks about how to use email authentication to stop phishing.[21] All three videos feature FTC staff attorneys who provide clear and direct guidance on these important cybersecurity topics. These videos, which businesses can find on the FTC's website and YouTube channel, have received thousands of views. Online websites like CIO.com and HealthCareITNews.com, as well as law firms, IT professionals, and marketing consultants have featured stories on their websites linking to the videos or refer to the advice they provide.

Finally, the FTC's video on the NIST Cybersecurity Framework[22] explains how the FTC Act's requirements relating to security fit within the NIST Cybersecurity Framework. Organizations like the International Association of Privacy Professionals and the Minority Business Development Agency, which is a federal agency charged with promoting business opportunities in minority communities, promote the video to their constituents and link to it from their websites.

D. Webinars and Presentations

The FTC offers numerous and highly-regarded webinars to train businesses on cybersecurity. In 2016, we conducted a series of cybersecurity webinars with NIST and the SBA. These webinars trained hundreds of small business owners, along with the professionals who help them, about

---

[19] Available at https://www.ftc.gov/news-events/audio-video/video/defend-against-ransomware

[20] Available at https://www.ftc.gov/news-events/audio-video/video/phishing-your-companys-good-name

[21] Available at https://www.ftc.gov/news-events/audio-video/video/stop-phishing-using-email-authentication

[22] Available at https://www.ftc.gov/news-events/audio-video/video/nist-cybersecurity-framework-ftc

the *Start with Security* principles and the NIST Cybersecurity Framework. In the past six months, FTC staff participated in four widely attended webinars NCSA hosted[23]. These webinars were part of a five-webinar series on the NIST Framework Principles and averaged between 800 - 1,000 registrants. Two more webinars are scheduled for spring of 2018.

The FTC often works with specific industry associations on webinars targeted to their particular concerns. These collaborations have been successful, since the FTC staff can tailor its presentations to the particular interests, needs, and reach of an industry association. For example, hundreds of tax preparers attended webinars offered by the National Association of Tax Professionals (NATP), which hosted FTC staff to train them in cybersecurity[24]. At these webinars, attendees learned about sound business practices, such as collecting only the personal information they need and disposing of it properly. They also learned about IdentityTheft.gov, the federal government's one-stop resource for identity theft victims. Tax preparers can refer clients to this website to report identity theft and get a recovery plan. Our collaboration with NATP continues with more webinars to come. Similarly, we collaborated with the American Escrow Association to offer a webinar on *Start with Security* principles for hundreds of escrow agents.

FTC Commissioners and staff also participate often in cybersecurity events throughout the country. During 2017, FTC staff gave presentations at dozens of events. Some notable events included the Conference of Western State Attorneys General, the International Legal Technology Association, the International Association of Privacy Professionals, the American Car Rental Association, the American Payroll Association, the National Association of Professional Background Screeners, and the Financial Services Roundtable. In addition, the FTC participated in a dozen local events around the country, in conjunction with NCSA and the Better Business Bureau (BBB). Through these events, the FTC was able to connect with local businesses and bring our cybersecurity materials and guidance to them.

Partnerships

The FTC collaborates on a regular basis with key federal agencies and other organizations that educate businesses about cybersecurity. These partnerships are important because they help amplify the cybersecurity education messages we develop. By collaborating with other organizations, we ensure that these messages spread broadly across the nation.

For example, we've worked closely with the Small Business Administration (SBA). This partnership has allowed the FTC to share its guidance on protecting sensitive information with

[23] Available at https://staysafeonline.org/resources/?filter=.resource-item.type-videos

[24] Available at https://www.natptax.com/EventsAndEducation/Pages/course-list-on-demand-webinar.aspx

small businesses nationwide. In 2016, the SBA hosted a series of webinars with the FTC and NIST, in which SBA leaders and small business owners learned about the *10 Cyber Mistakes You Can't Afford to Make*. In 2017, FTC staff gave presentations at two Cybersecurity Symposiums: one in Boston, hosted by the SBA's Massachusetts District Office, and one in Portland, Maine, hosted by SBA's Maine District Office. Also in 2017, the FTC's Western Regional Office participated in a Small Business Conference in the Los Angeles area, sponsored by the SBA's Santa Ana District Office. And on May 9, 2017, *The Hill* ran an op-ed, *How America's small businesses can become cyber savvy and scam-free*,[25] in which Acting FTC Chairman Ohlhausen and SBA Administrator Linda McMahon discussed how both agencies are working together to help small businesses become more cyber savvy.

The FTC is the current Chair of the Cybersecurity Forum for Independent and Executive Branch Regulators. The Federal Communications Commission, the Federal Energy Regulatory Commission, the Food and Drug Administration, Department of Homeland Security, U.S. Coast Guard, Department of Transportation/Federal Aviation Administration, Department of Treasury, National Association of Insurance Commissioners and the National Institute of Standards and Technology, among others, are part of this collaboration. The objectives are to share best practices, explore ways to align approaches to enhance cybersecurity protections, and establish processes to encourage coordination and consistency.

We also work closely with Congressional staff. Acting Chairman Ohlhausen testified before the House Small Business Committee on March 8, 2017, where she spoke about the FTC's cybersecurity resources for small businesses. After that hearing, Chairman Chabot directed Committee staff to post three FTC publications on the Committee's website[26]. This is just one example of the many groups that use and customize FTC materials to educate businesses about cybersecurity. We also provide materials to Congressional district offices and often participate in outreach events held by Congressional staff in districts across the country.

In addition, the FTC collaborates regularly with National Cyber Security Alliance (NCSA). This organization, which works closely with the Department of Homeland Security (DHS), has been an instrumental partner in the FTC's outreach efforts on cybersecurity. NCSA has invited three FTC Regional Directors to participate in its CyberSecure My Business Workshops. NCSA also regularly promotes FTC messages to the public and their partners through their communication channels and social media. The FTC serves on NCSA's federal partner working group.

The National Alliance of Women Business Owners has been another partner organization on several occasions, allowing us to bring the FTC's cybersecurity advice to their membership. They have published two articles in their e-magazine, *ONE*, featuring the FTC's information for

---

[25] Available at http://thehill.com/blogs/pundits-blog/technology/332484-how-americas-small-businesses-can-stay-cyber-savvy-and-scam

[26] *Building Security in the Internet of Things*, *Data Breach Response*, and *Protecting Personal Information*. Available at https://smallbusiness.house.gov/resources/committee-publications.html

business. FTC staff also presented at their annual conference in 2016 and in 2017. The BBB is another regular partner. Its *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

In the spring of 2017, Acting Chairman Ohlhausen directed the agency to create FTC.gov/SmallBusiness, a new website that helps small businesses and non-profit 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, *Small Business Computer Security Basics.*[27] The article includes tips to help protect a company's files and devices, train employees to think twice before sharing account information, and keep wireless networks protected. The article also gives information on what to do if a hacker gets into a small business's system.

B. Small Business and Cybersecurity Roundtables: Engage, Connect, Protect

Between summer and fall of 2017, the FTC hosted five roundtable discussions with small business owners in collaboration with the SBA, NCSA, and other federal and local partners.

The goal of the Small Business & Cybersecurity Roundtables: Engage, Connect, Protect[28] was to listen to business owners and non-profit organizations employees and managers, to learn from them about challenges they face when dealing with cyber threats and security, and to hear their ideas on how the government can help them.

---

[27] Available at https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics

[28] The FTC first announced the initiative on the blog post *FTC to Small Business: Gather Round*, available at https://www.ftc.gov/news-events/blogs/business-blog/2017/07/ftc-small-businesses-gather-round.

The roundtable discussions took place in Oregon, Iowa, Ohio, Delaware, and North Carolina. There were 10-15 owners and employees of businesses and non-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, embroidery and printing services business owners, gas station consultant, accountant, executive coach, graphic designer, attorney, bookkeeper for a non-profit 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 and would appreciate guidance on what to look for when shopping for it.
- Vendor security also is a concern. Some participants suggested the government should provide a list of questions to ask vendors to make sure their systems are secure and are not going to expose customers' or employees' information to a data breach.
- Other concerns had to do with implementing policies on the security of removable data, keeping backups up-to-date, and the physical security of business equipment, including mobile devices.

Finally, some participants asked us to provide free information that business owners could share with employees to help train them on cybersecurity topics. Most participants agreed that any materials, including videos, should include action-oriented advice that is easy to understand and apply. Some asked for information in Spanish as well as English. They also noted that they appreciate materials that are engaging and educational, and that raise awareness of cyber threats in a way that will help people behave more cautiously.

Plans for a 2018 Small Business Cybersecurity Education Campaign

Based on the lessons learned in the roundtables, 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 of training materials for small businesses and their employees

The FTC and campaign partners will develop and distribute materials that provide the information small business owners seek about cybersecurity and protecting data. We will develop a series of 10-12 modules, or sets of information, on topics small business owners told us they care about. Each module will include a short written description of a cybersecurity challenge, and advice for dealing with it. The campaign also will include short videos, presentation slides, and other materials.

The materials will be appropriate for small business owners and managers to share with employees. These plain-language materials will recognize and convey that businesses should take measures that are reasonable given their size and industry, the threats they face, and the types and amounts of data in their care. Potential topics include:

1. Phishing
2. Ransomware
3. Protecting mobile devices
4. Understanding the NIST cybersecurity framework
5. Cloud security
6. Wi-fi
7. Email authentication
8. Physical security (at the office and on travel)
9. Security of removable media, backups
10. Scams: tech support, imposters
11. Vendor security
12. Business IDT (aka "business email compromise")
13. Cyber basics
14. Cyber insurance[29]
15. How to compare offers of web hosting services.

[29] The FTC does not have jurisdiction over the business of insurance as regulated under state law. We have partnered with the National Association of Insurance Commissioners (NAIC) to bring cyber insurance information to small businesses.

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 FTC staff belongs to, we will approach our counterparts at other key federal agencies to create messages that other agencies can adopt as their own. In addition, in coordination with DHS' IT Sector Small and Midsize Working Group, the FTC has been helping to find ways to encourage the use of the NIST cybersecurity framework in the small business community. Agencies will have the opportunity to brand the materials with their logo or seal, adopt information from the campaign to fit their ongoing programs, or target specific industries, based on their missions.

C. Partner with the private sector

As described above, the FTC and its federal partners have developed a productive working relationship with industry associations and other partners in the private sector, including the NCSA, the Better Business Bureau, the U.S. Chamber of Commerce, and many other organizations. The FTC and its partners will continue to distribute campaign materials to small businesses through these organizations and other intermediaries. Campaign materials will be available online. Printed materials are available free from the FTC's bulk order website at FTC.gov/Bulkorder. In addition, the campaign will be associated with the Stop*Think*Connect national public awareness campaign managed by DHS and NCSA.

Conclusion

The FTC has been providing information and cybersecurity guidance to businesses through education and outreach efforts. We've built successful partnerships with industry associations, trade groups, and other government agencies to help businesses of all sizes improve their cybersecurity. Building on those current business education efforts and the knowledge staff gained from our recent small business roundtables, the FTC will create materials that help small businesses navigate the world of cybersecurity with more confidence. We will ask other federal agencies and national, regional, and local organizations to help us disseminate these materials to ensure business owners and employees have access to them and can learn from them.