DIGITAL SECURITY 101 FOR SMALL BUSINESSES

Brought to you by intel

WORLD PASSWORD DAY2017 | TECHSPACULAR!

> Marketers and their employers are missing a potentially powerful brand- and business-building opportunity: leveraging online security measures as a way to build trust with shoppers, which will ultimately lead to increased sales.
>
> **— Harvard Business Review**

If you're a small business, you probably work very hard to keep your customers happy. But good customer service goes beyond a friendly hello or prompt service. Today, the most forward-thinking companies are taking measures to protect the sensitive data entrusted them by customers.

Just because you may not have a dedicated IT position on staff doesn't mean you can't take steps to protect your customer's data.

More than anything else, security is about good habits. Approximately 43% of cyber attacks are against small business — here's how you can protect yourself, and your company.

PROTECT YOUR DATA

SECURE YOUR TEAM

GET STARTED

PROTECT YOUR DATA

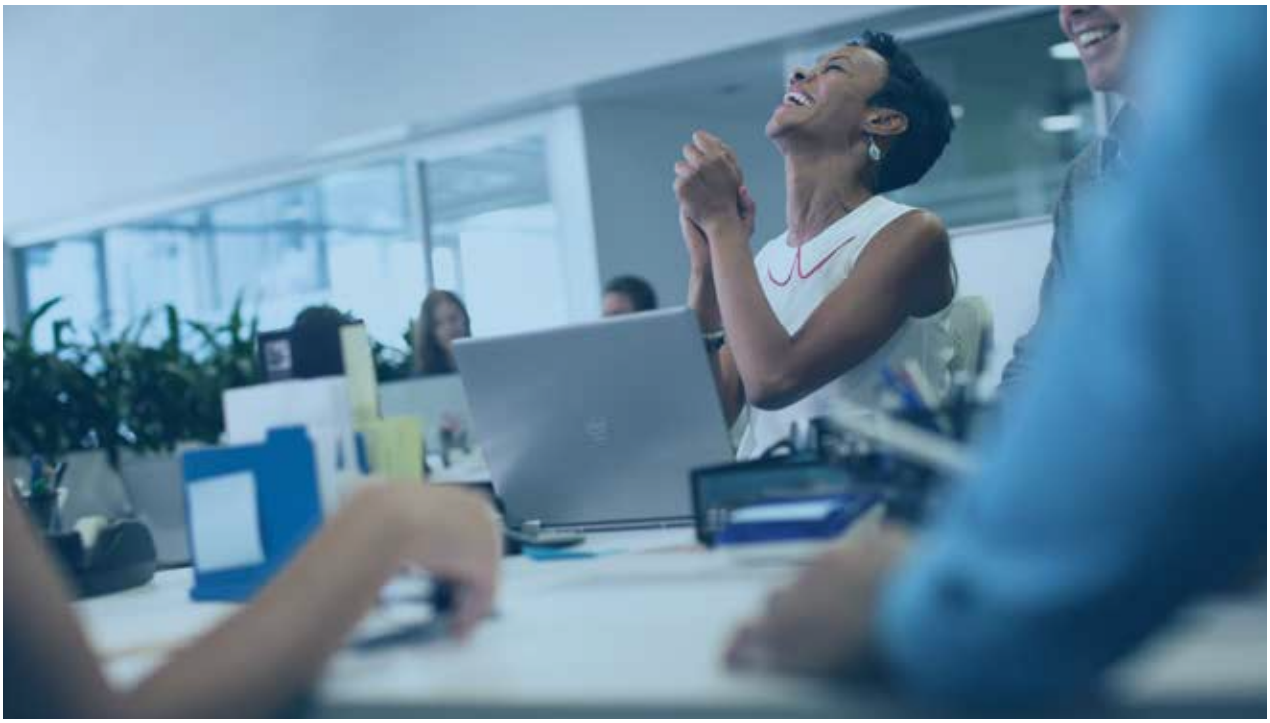
> “Better be despised for too anxious apprehensions, than ruined by too confident security.
>
> **— Edmund Burke, Author and Political Theorist**

NETWORK

Network threats are continually evolving. You can stay ahead of today's attackers with innovative security solutions that detect, analyze, and block advanced threats like ransomware before they reach your employees on the web, email, and social platforms.

TIPS

- Keep your machine clean by always having the most up to date versions of your security software, operating system, and web browser.
- Be sure a firewall is in place to keep your network private.
- Regularly backup all important business info and store offsite or in the cloud.



WEBSITE

Ideally, security procedures should be integrated into your website as it's being planned and developed. After development, performing regular penetration tests and vulnerability scans against your websites is a must to detect critical security issues before real hackers do.

TIPS

- Limit the amount of sensitive information uploaded to your site and encrypt all that is uploaded.
- Remove or disable any unnecessary services on your server.
- Regularly backup all site data and store offsite or in the cloud.
- Update all server software to the most up to date versions.

WI-FI

If you offer Wi-Fi to employees or visitors be sure it is secure and protected.

TIPS

- Offer separate networks for employees and anyone else needing internet access.
- The employee network should be encrypted, network name not broadcasted, and the network restricted to specific devices.

ACCOUNTS

If you've read the news at all in the last few years, you'll know that businesses are prime targets for security breaches. But small businesses are at even more of a risk for cybercrime. Why? Without a dedicated defense, like an IT or security department, they make an easier target.

Your first line of defense is a strong password protected by two-factor authentication. Without that, the websites you use to power your business — email, e-commerce, accounting, even social media — are prime targets for a takeover.

TIPS

- Use unique passwords for each account. (Getting a password manager can help relieve the burden of having to remember them all.)
- Don't share your passwords between employees on chat or email. (Password Managers also provide secure ways to share passwords between employees.)
- Add additional layers of authentication on as many accounts as you can. Go to passwordday.org to learn more about Layering Up your Logins.

SECURE YOUR TEAM

> “ Amateurs hack systems, professionals hack people.
>
> **— Bruce Schneier**

ENLIST YOUR EMPLOYEES

The old cliché “a chain is only as strong as its weakest link” is very true when it comes to security. Company employees (and even CEOs) have replaced software exploits as attackers’ favorite way to infiltrate your business. Enlist your employees in the cause. And make security a part of your workplace culture.

TIPS

- Develop an ongoing education program that covers the security basics for passwords, email, browsing, and social engineering.
- Run weekly, ongoing phishing simulations.
- Send regular reminders of security topics and company security policies.
- Consider adopting password management software.

PROTECT THEIR DEVICES

Most small businesses use mobile phones, laptops, and tablets as a way to increase employee productivity. Although extremely convenient, they can offer a significant potential threat. Mobile devices are often lost or stolen which can lead to data loss or a security breach. Policies and procedures need to be put in place to increase mobile device security.

TIPS

- Password protect and install security software on every mobile device that has any company email or information.
- Encrypt mobile device data.
- Have reporting procedures in the event of a loss.

PRACTICE SAFE CLICKING

Most cyber attacks require a user to click something: a malicious link in an email or text, the install button of a virus disguised as legitimate software, or just a dangerous attachment. It is estimated that approximately half of all email is spam, phishing attempts, or other unwanted messages. It is the most prevalent way of spreading malware and imperative that precautions are taken to keep it safe and secure.

TIPS

- Install security software to automatically identify and block malicious messages.
- Enable email encryption.
- Create policies for employees on how to identify safe and unsafe links in email or on the web.

REFRESH YOUR TECH

Microsoft reports that the average age of today's PC is 4.4 years old — close to what many experts consider to be a 5-year maximum life for computers. If it's time to refresh your company's tech, make sure you consider the hardware security features that computer and server manufacturers are offering.

TIPS

- Look for hardware security features like secure biometrics, built-in 2-factor authentication, and secure enclave technology built into the computer's processors.
- Consumer Reports now measures the privacy and security of the products, apps, and services they review. Make sure to use this to help inform your purchasing decisions.

GET STARTED

> “There are risks and costs to a program of action — but they are far less than the long-range cost of comfortable inaction.
>
> **— John F. Kennedy**

CELEBRATE WORLD PASSWORD DAY!

The first Thursday of May each year is designated as World Password Day — the perfect time to educate your company and clients about data safety and identity theft protection.

As more and more sensitive data is stored online, the effects of cybercrime grow more significant each year. World Password Day can be a great way to keep your employees up to date about strong authentication standards.

This year, celebrate in your office by pledging to #LayerUp your logins and by sharing educational tips, graphics, and materials. The website below has free materials available that are updated annually.

Treat every day like Password Day. Visit us at https://passwordday.org

NEXT STEPS

Feeling overwhelmed? Here are some resources.

If you don't know where to start with improving your business' online security, check out these resources, or find an expert in security and privacy for small businesses.

- Intel's Digital Security page has great information on protecting your logins. https://digitalsecurity.intel.com
- The Small Business Association has a wonderful cybersecurity tool to kickstart your cybersecurity plan. http://bit.ly/1xszK4c
- The National Institue of Standards and Technology also has small business cybersecurity on lock. Check out their comprehensive guide to all things security here. http://bit.ly/2gtfw5e
- Consumer Reports is a great resource when upgrading your hardware to the latest technology. They now rate products for security and privacy. https://www.consumerreports.org

Content generously provided by Techspacular℠, a consultancy that specializes in helping small and medium businesses with information security. Find them at https://www.techspacular.com