

A hand holding a silver smartphone over a laptop keyboard. The background is a blurred office setting.

**Entrust<sup>®</sup>**

# cybersecurity 101

## For Small & Medium Businesses

**entrust.com**

**+1-888-690-2424**



Entrust



EntrustSecurity



Entrust



# easy security tips for SMBs

Unfortunately, end-users are often left out of the conversation when looking for ways to bolster security across the enterprise. A lack of training and education often play a big part in leaving end-users exposed to nasty forms of malware that can infiltrate an operating system and wreak havoc over a company network.

In fact, a recent study by Trustwave<sup>1</sup> indicates that up to 14.4 incidents of data loss per year can be attributed to employee negligence. Further, 15 percent of enterprises claim to have reported an insider breach with malicious intent.


IT managers need to recognize that until all end-users are caught up to speed with basic cybersecurity training, attacks will continue to pose major problems.

With so many cybersecurity factors to pay attention to, where does one begin to assess ways to prevent breaches from occurring?

Here is a look at some easy tactics that can be deployed by end-users across your business to make sure that cybersecurity remains a top of mind throughout the year.

1. Trustwave 2013 Trustwave Global Security Report (2013) at <https://www.trustwave.com/Resources/Library/Documents/2013-Trustwave-Global-Security-Report/>





# one

## Keep Operating Systems Updated

One of the most important aspects to ensure digital safety when sharing information with end-consumers across your enterprise is to remind — or require — that end-users ensure their operating system is updated.

If OS updates aren't managed by your organization's IT department, it is strongly advised that end-users enroll in built-in automatic updates so that they are always on top of the latest software.

This will prevent third-party criminals from gaining access to private information via security voids that have already been patched.

# two

## Ensure Browsers Are Up To Date

Internet browsers are constantly in need of updates, and running old or out-of-date browsers can pose serious security risks. That's because old browsers become less stable as they age, and as a result, viruses and various forms of spyware can gain access to a computer when users unknowingly click on malicious links and download malware or other nefarious viruses.

Outdated browsers also run the risk of playing part in a number of different types of man-in-the-middle attacks, in which a third party enters a computer and facilitates attacks silently against other machines — or groups of machines.

Check to see that browser settings are up to date, and always restart the browser after the updates occur in order to make sure that changes are installed properly.

# three

## Scan PCs For Malware And Viruses

Scanning PCs for malware and viruses should be treated like regularly visiting the doctor. If you haven't done it in a while, you are probably overdue. It is vital that end-users recognize the constant threat of malicious software and scan regularly to avoid getting hit with an attack.

Jason Soroko, manager of security technologies for Entrust, explains that's it critical to remain prudent in defending against advanced malware. Each evolution is becoming more resilient than the previous generation.

"Malicious activity is much more difficult to detect than we have been led to believe. By securing the identity, we have the means to defend against the most sophisticated threats," said Soroko.

In response, enterprises must understand that security — such as strong authentication and mobile-based identities — is no longer a luxury but a must-have in 2014. These threats are real, and they are lurking in cyberspace.

For end-users, it is vital to scan regularly, using free software such as Malwarebytes or Microsoft Security Essentials (MSE), which are both capable of detecting and eliminating threats over a network. (As always, use of the aforementioned antivirus software is the responsibility of the reader.)

**"Malicious activity is much more difficult to detect than we have been led to believe. By securing the identity, we have the means to defend against the most sophisticated threats."**

**-Jason Soroko,  
Manager, Security Technologies  
Entrust**





A hand is holding a white tablet. The screen shows a data visualization with a bar chart on the left and a 3D pie chart on the right. The background is a soft-focus image of a person's hand and the tablet.

# four

## Clear Out Spam Folders

The spam folder is where the majority of phishing emails reside. Most email clients automatically delete spam emails after a set period. However, it's a good idea to go through the spam folder more frequently to delete suspicious emails so they are not lurking on the system.

Educate users on what phishing emails and spam are, and encourage them to take time to report or block emails from suspicious senders or known phishing sources.

Make sure they know not to open spam emails before they delete them — falling victim to a phishing email could install malware, spam a user's contacts list, or steal financial information.

# five

## Upgrade To Stronger Passwords

Make sure to change passwords and security questions frequently to lower the chance of social media or email accounts being hacked.

Strong passwords are more than eight characters long, do not contain names or complete words, are unique from other passwords, and contain a mix of lowercase and uppercase letters, numbers, and special characters. Users may want to consider a secure password management program that helps keep passwords organized.

Also, consider multifactor security steps to bolster passwords and protect against hacking. Multifactor authentication could use generated passwords and biometrics, or PIN numbers to unlock a device.



## **Invest In Biometrics To Protect Your Smartphone Applications**

Smartphones are extremely useful, but today's smartphone apps also tend to contain a large amount of sensitive information, from financial data to corporate emails to photos, schedules, spreadsheets and medical information.

If the device is lost or stolen, a user never knows if an unknown party might be using apps on the device to make purchases and perform other activities. Biometrics can change all that.

Biometrics protect smartphone applications and sensitive data by requiring a unique authentication to access the apps on the device, such as a fingerprint or voice authentication.

For example, Apple's iPhone 5s debuted TouchID, built-in fingerprint scanning technology that uses a user's unique fingerprint rather than a PIN number to unlock the device.

Other companies now have voice recognition software to unlock apps and databases. The advantage of biometrics is that they are affordable, and can go a long way toward improving smartphone security for consumers.







# seven

## Remove Unneeded Plug-ins/Add-ons

It happens to many users: they install software and forget to uncheck the “install toolbars” or “install plugin” box. Or they click on an ad and suddenly find something has been planted on their system they didn’t want. Some add-ons and plugins for desktop browsers are valuable, especially if they come from a service you trust and you use them regularly.

However, many are rife with malware and adware, and send users to an unsecure site that may install malicious software or spyware on the system if used. It’s a smart idea to remove all add-ons that aren’t critical. This will help protect the network from potential malware, as well as uncluttering the browser and increasing its speed and performance to make it more functional.

# eight

## Understand SSL Certificates

It’s never too late to understand how SSL certificates work. SSL certificates act like credentials for websites, showing that a website is safe and that it protects sensitive information. When you connect to a site protected by an SSL certificate via your browser, the server sends back information letting you know that the connection is secure.

Ensure your customers know to look for a closed padlock in the browser window. This shows that a site’s SSL certificate is active and up-to-date. In addition, the letters “HTTP” at the beginning of the address will change to “HTTPS” when the connection between the server and the browser is secured by SSL. If the browser address bar turns from white to green, it means the website is using Extended Validation SSL.

Ready to Secure Your Site?  
Try Entrust EV SSL.

**Buy Now**

# nine

## Block Or Report Phishing Attempts On Social Channels

The latest venue for phishing scams is social media. Users may see a post, chat or private message from a social media contact that doesn't seem quite right, urging them to click on a link.

One popular Facebook phishing/spam message, for example, asks the user to look at photos of a friend's burned living room after a fire. Once the link is clicked, it installs malware on the system.

Inform end-users not click to suspicious links in status updates, tweets, chats or private messages on social networks. This rule also applies to online ads and sponsored posts.

Instruct users to block and report spam and phishing, and to report it to the social media site. Users should also delete social media contacts whose accounts have been hacked, and delete any old or unused accounts to decrease the likelihood of them being taken over by cyber criminals.







# Security That Works for You

## Simplify Your Security

You've got your day-to-day business to run. Partner with a trusted security vendor to help you manage any or all parts of your new security plan. From simple SSL certificates to strong authentication controls, Entrust can tailor a security strategy that's perfect for your business.

## Proven Security for Less

Our identity-based security solutions are designed to go with the evolving needs of your business. Start small and only pay for what you need today. As your requirements change, our platforms easily scale as the security landscape shifts.

## One Trusted Vendor

Entrust wants to make it easy. That's why we can provide your business with all the necessary security solutions that are proven to protect organizations of all sizes in every vertical. And we even offer simple cloud management so you can focus on what's important — your business.

Your small- or medium-sized business runs on hard work, dedication and loyal customers.

But your size shouldn't exclude you from using the proper security technology to protect online customer identities. It's now part of your plan to help build trust, secure transactions and drive business.

Let's put your ideas into action with specific security strategies that are both proven and cost-effective for SMBs.



[entrust.com](https://entrust.com)

+1-888-690-2424