Computers and stuff.

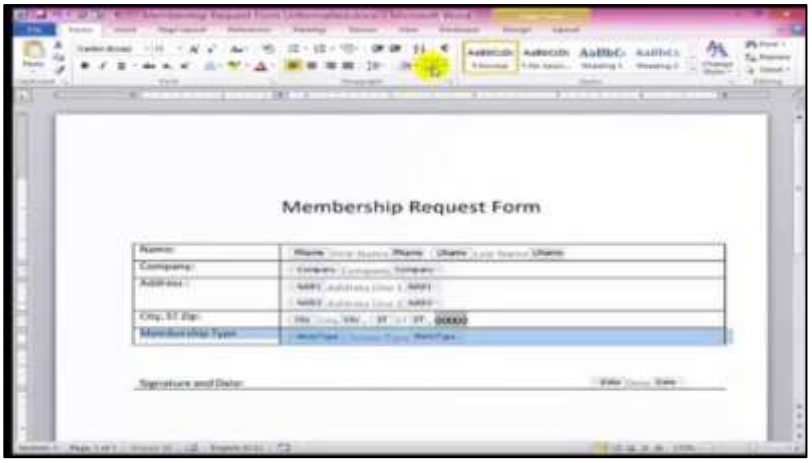
Sam Houliston.

Contents.

Create a Form in Word.

Creating a fillable Form in Word is easy, here's how.

You need to create an electronic form that's easy for people to fill out but that can't be modified by anyone but yourself. No problem. Microsoft Word can handle that challenge. You can create a form complete with the necessary fields, graphics and other content. You could create it from scratch but you'll find it easier to start with a built-in template for a form. From there, you customize if necessary.



You can control or limit the type of content people can add to a specific field and you can protect your form so people can't alter it beyond filling in the fields.

Why would you want to?

- You may work at a company where you need to generate electronic forms for job applications, employee surveys, confidentiality agreements, or expense reimbursements.
- Maybe you work for a school that uses permission forms, student evaluations, emergency contact information, or back-to-school checklists.
- Perhaps you work for a doctor or hospital and need forms for patient registration, medical surveys, or patient progress.
- Or maybe you want to create and send forms to people for meeting or party planning, charity or volunteer functions, or club membership.

This help topic relates to Word 2016, but you can create a form using the same steps in any of the prior few versions of Word.

This information can help if you're trying to create a form based on a template.

Open Word. You can access templates one of two ways depending on your Word configuration. If Word is set to display the Start screen upon launch, the page of template thumbnail images appears. If Word is set to bypass the Start screen, click on the File menu and select New to view the list of templates. By default, Word shows you thumbnails for featured templates. You can click on a specific category at the top, such as Business, Industry, Personal, or Education, to focus the list, but your best bet may be to search for a template. Start by typing the word forms in the search field at the top and pressing Enter. You can now browse through the list of thumbnails to look for the right form.

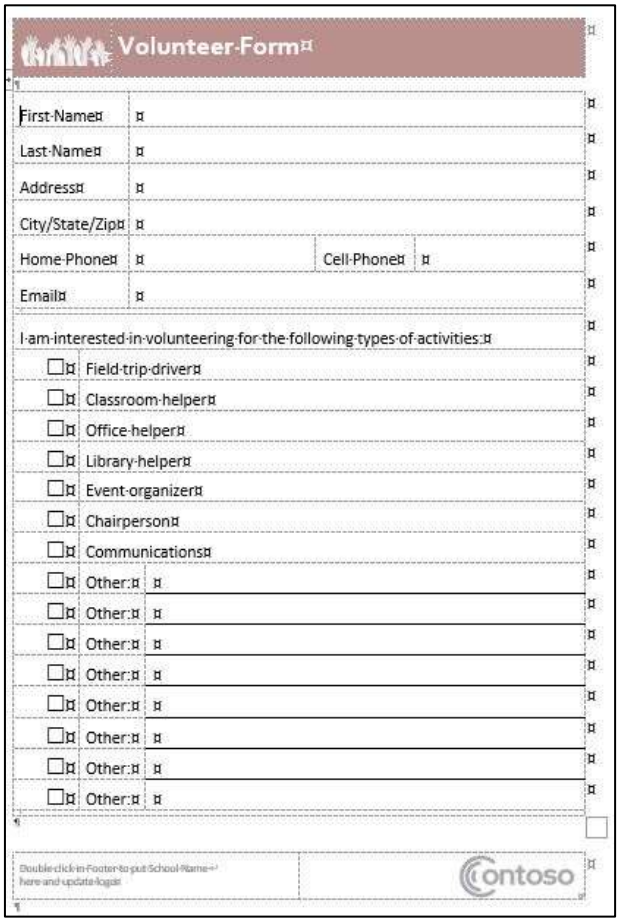
Let's say you need a Volunteer Form, you'll find one there, just click it and then click Create

Scroll down the page to review the template. Notice that it already includes the necessary fields, some of which you fill out or replace and some of which people who receive the form fill out.

Many forms contain some type of graphic, such as a company logo. In the Volunteer Form it is just to the left of the words in the heading. Click on the image and then click on the Graphics Format menu to access the Picture Tools Ribbon. Click on the button to Change Picture (far left) and now you can upload the appropriate image. You can then use the tools on the Picture Tools Ribbon to tweak and fine-tune the image.

Click on the first piece of text that you need to change, such as Volunteer Form. You might want to change it to Radschool Volunteer Form, if so, highlight it then just type the replacement text, the current text will disappear. If you want to change the font or colour of the text, just select the Home menu, highlight the text and make your changes.

You can change any text on the form that you wish, just highlight the text you wish to change and type in the replacement. You can add rows or columns, just click where you want to add either a row or column, right click then select Insert and click what it is you wish to add. You can leave other lines or paragraphs of plain text as they're written or rewrite them. You can delete any text or other content that you don't want in the form.


Volunteer Form

First Name			
Last Name			
Address			
City/State/Zip			
Home Phone		Cell Phone	
Email			

I am interested in volunteering for the following types of activities:

- ☐ Field trip driver
- ☐ Classroom helper
- ☐ Office helper
- ☐ Library helper
- ☐ Event organizer
- ☐ Chairperson
- ☐ Communications
- ☐ Other:
- ☐ Other:
- ☐ Other:
- ☐ Other:
- ☐ Other:
- ☐ Other:
- ☐ Other:
- ☐ Other:

Double click in Footer to put School Name here and update logo

Contoso

You could find that some forms have two fields on the one line, you'll find it much easier to protect your form if you only have one field per line. If there are two in the template, add another row and move the second one down a row. See below:

The form at right is the form as it is when you load it from the Template library, run your mouse over it to see how to change it so there is only 1 field per line.

You can also add text or other content to the form. The way you do this depends on the form and the type of content you add. In some cases, you can simply add a sentence or paragraph to a form. Many forms are designed using tables, so you might add an extra row or column to make space for a new piece of text.

Notice that some of the text and other items display a grey background when you click on them. Those are known as content controls, which are designed for the people who receive your form to fill in specific fields. Content controls can be straight text boxes, but also check boxes, date pickers, and drop-down lists.

After you've set up your form, you now need to protect it. You want people to be able to fill out the form in the appropriate fields but not change any of the controls or content you set up. The quickest way to do this is as follows:

- Click on the Developer menu and click on the icon to Restrict Editing.
- At the Restrict Editing pane on the right, check option 2 for Editing restrictions and then select *No changes (Read only)*
- Select the fields and areas of the form where people can change or fill in information. You can use Ctrl or Shift to select multiple areas in one shot. Also, you may find it helpful to click on the Paragraph symbol icon on the Ribbon to see the hidden formatting symbols. Click he box against *Everyone*. Click on the button to *Yes, Start Enforcing Protection*, type and then retype a password.

Now, people who receive the form should be able to modify the fields you selected but not any other parts of the form.

If you want to make any changes to the form, click *Stop Protection* (at the bottom of the window at right) then type in the password. This unprotects the form and you can make any changes.

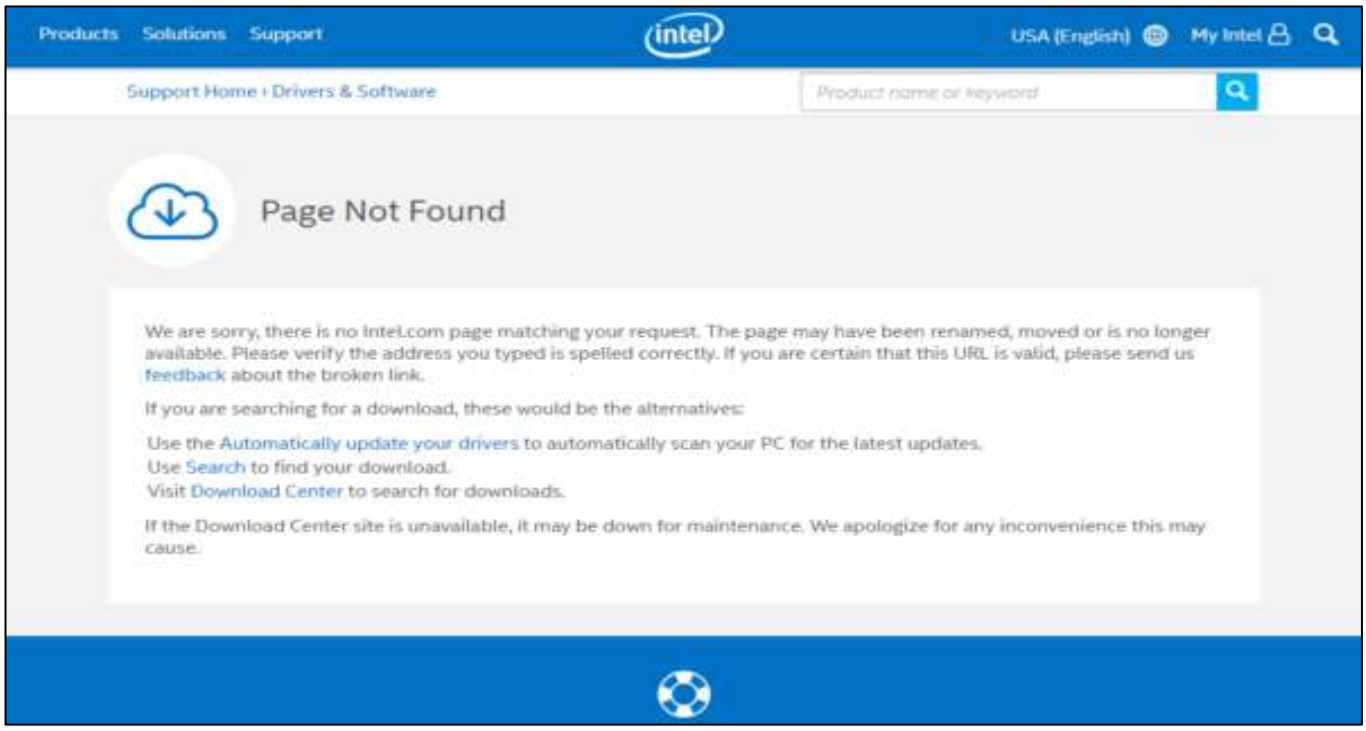
Q. What is the biggest lie in the entire universe?
A. I have read and agree to the Terms and Conditions".

How to check if a website and its files are malicious.

A significant amount of malware infections and potentially unwanted program (PUP) irritants are the result of downloads from unreliable sources. There are a multitude of websites that specialize in distributing malicious payloads by offering them up as something legitimate or by bundling the desired installer with additional programs.

In November 2019, Intel removed old drivers, BIOS updates and other legacy software from their site. While this software relates to products released in the last century and early years of the 2000s, many users still rely on old Intel products and have been left scrambling for specific downloads.

Users that follow older links to certain drivers and updates will find this instead:



Following the links to search the site or the download centre only leads users around in circles, those downloads are gone. While some might argue that it is Intel's right to remove drivers and updates after a decade, others understand that whenever legacy software is abandoned, a security nightmare ensues.

When users can no longer download files from official sources, desperate people will roam the Internet for a place where they can find the file they need. And what they usually find instead are malicious websites and downloads.

Malvertising using popular downloads.

Habitually, threat actors find out which search terms are gaining in popularity as users seek out terminated software downloads and try to lure searchers to their site. They will use SEO techniques (Search Engine Optimization) to rank high in the search results or may even spend some dollars to show up in the sponsored results for certain keywords. They can hide their malware in malvertising in the form of downloads or even drive-by-downloads, in which users needn't install a single file, only visit the site, to be infected.

After all, a victim that is desperately looking for a file he needs to get a system up and running again is really all a malware peddler could wish for. All they have to do is make the user of the site believe they have found the file they are looking for. Once they are convinced, they will download and install the alleged driver all by themselves. All the threat actor has to do is upload the malware under some convincing filename and attract visitors to the site. This is basically the same modus operandi that you will find in use when people go looking for cracks and keygens.

So, what can users do to avoid falling victim to such a scam? A couple of things, as it happens. Malwarebytes will provide you with some checks you can do before you visit the download site. And there are some checks you can perform before you run the downloaded file, too.

Checks you can perform to assess the website

When you have found a site that offers a file for download, there are a few actions you can take to check whether the site is trustworthy. They are:

- Check for the padlock next to the URL.
- Read third-party reviews of the website.
- Use a trusted antivirus or browser extension, such as Browser Guard.

Checking for the presence of the green padlock is a good start to ensure a site has purchased a security certificate, but it's also not a guarantee that the website is safe. SSL certificates are cheap, and your neighbourhood cybercriminal knows where to get them practically for free. If you click on the green padlock, you can find out who issued the certificate and for which site.

There are many websites that offer reviews of download sites and domains, and while many of these sites are reputable, they tend to fall a little bit behind in adding Internet newcomers. A cybercriminal can afford to dump a domain like a hot potato once it has racked up too many bad reviews, then purchase a new site from which to run his scheme. In short, you can trust reviews about sites that have been around for a while, but the lack of reviews for a site could mean they only started or they may be up to no good.

Some cybercriminals are brilliant programmers. Most are not. But all the successful ones have one skill in common, they are well-versed in tricking people. So! don't accept a website as trustworthy just because it features logos of other trustworthy companies on its pages. Logo images are easily found in online searches and they could be planted on the site for exactly that reason, to gain the visitors' trust. Logos could also be stolen, unauthorized, or handed out for different reasons than you might expect.

Some browsers and some free applications warn you about shady sites—especially sites they know to be the home of malware and scammers. Malwarebytes Browser Guard, for example, can be installed on Chrome and Firefox, adding to the browsers' own capabilities to recognize malicious domains and sites.

How do I filter possible malware from the downloaded files

There are some methods you can use to weed out the bad boys in your download folder:

- Compare the checksum to the original file
- Look at the file's digital signature
- Run a malware scan

A checksum is a sequence of numbers and letters used to check data for errors. If you know the checksum of the original file, you can compare it to the one you have downloaded. Windows, macOS, and Linux have built-in options to calculate the checksum of a file.

The digital signature of a Windows executable file (a file with an .exe extension) can be verified after the file has been downloaded and saved. In your Downloads folder, right-click the downloaded .exe file and click Properties. Here you can click on the Digital Signatures tab to check whether the downloaded file is signed by the expected party.

Finally, use your anti-malware scanner to double-check that you are not downloading an infected file. You can also use online scanners like VirusTotal, which will also provide you with a SHA-256 hash for the file and save you the trouble of calculating a checksum.

Much ado about what?

All this may seem like a lot of work to those who habitually download files without a worry in the world, however, even the most practiced downloader eventually has their moment of truth—when that downloaded file wrecks their computer or all those bundled applications are harder to remove than expected.

People who download all the time have better instincts about which sites to trust or not, but that doesn't mean they can't be fooled. From experience, they know the sites that offer malware under a different filename from the sites that offer clean files. But sometimes, we reach for the shiny golden delicious and, once we take a bite, discover it has a worm.

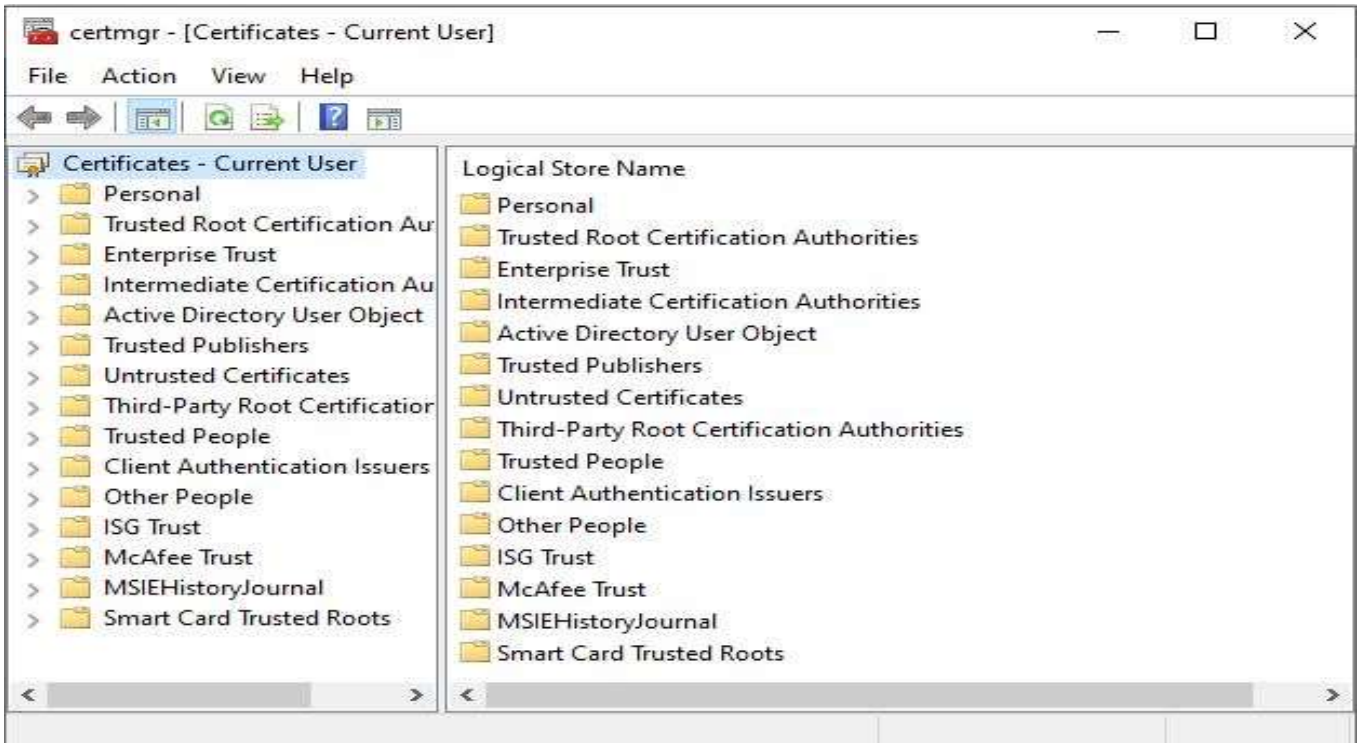
Even if you follow all these pointers to the letter, it is still riskier to download files from unknown sites than it is to download from the company that made them. So, we would like to urge companies to keep their "old files" available on their own site, even if the number of downloads has dwindled.

Stay safe, everyone!

A roadrunner's top speed is 20 mph while a coyote can reach speeds of up to 43 mph.
My whole childhood was a big lie.

Security Certificates – What are they?

First, it helps to take a look at your own certificates. Go ahead and open the Microsoft Certificates Management Console. You can do this by typing ***certmgr.msc*** in the search field of your start button. You will need to click “Run as administrator”.



You should see an overview of your certificates divided up into categories. The most used and usually the most important categories are Trusted Root Certification Authorities and Untrusted Certificates.

What are these certificates?

Root certificates are a method to prove that a communication you are receiving (from a website, by mail, or otherwise) comes from the source that it claims to be. This is done by public key encryption to establish a trust between the holders of the public and the private keys, but since it would be impossible to store certificates for every site we’ve ever visited or wish to visit, the system of certificate authorities (CA) was set up. To establish trust that a certificate is genuine, it is digitally signed by a root certificate belonging to a trusted certificate authority. Operating systems and browsers maintain lists of trusted CA root certificates so they can easily verify that they have been issued and signed.

You may have seen prompts warning you about a website’s security certificate, or as in the example below, a mismatch between the certificate and the name of the site:

The image shows which checks have been made before allowing a free exchange of information:

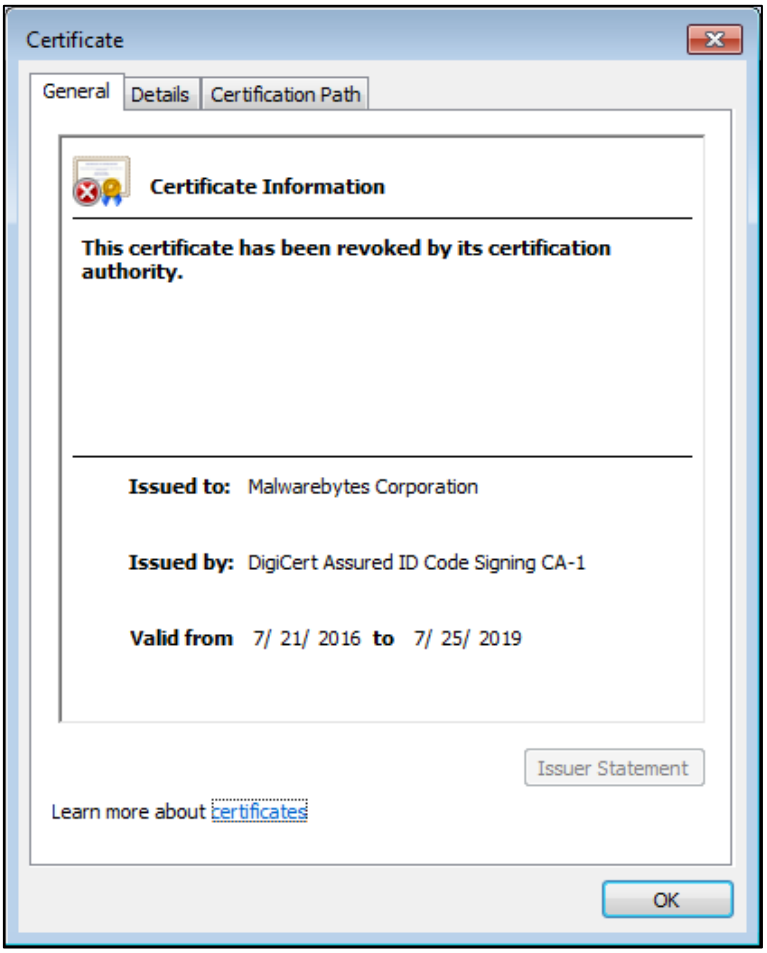
- Can we trust the source of the certificate?

- Is the certificate still valid? They all have a starting and an expiration date.
- Is the name valid, and does the name on the certificate match the name on the site's certificate?
- Is the signature strong enough?

Another important check needs to be done, however. Has the certificate been revoked? Sometimes the CA revoke certificates, mainly because the certificate, or the private key, has been stolen or compromised. This check is made against the Certificate Revocation List (CRL), which is a system that unfortunately has some flaws, meaning sometimes the check is not completed.

Untrusted certificates.

Certain types of malware place certificates in the Untrusted category, which basically disables users from downloading and using security software to remove the malware. At right you can see that the Malwarebytes certificate was placed in the Untrusted category by the ***Wdfload*** malware.



This certificate, however, has nothing to do with Malwarebyte's website, instead, it's associated with their software. With the certificate in the Untrusted category, this is what you will see if you try to run Malwarebyte's software.

Even though the CA (DigiCert) did not revoke their certificate and can still be found under their Trusted Root Certification Authorities, the Malwarebytes certificate was listed as revoked by the malware. The certificate shown above must be removed from the Untrusted category before the software can be used again.

So there you have it: a brief explanation of how security certificates work and how malware can abuse the certificates system to block you from downloading and/or running your favourite software.

"The trouble with quotes on the Internet is that you can never know if they are genuine"
Abraham Lincoln

What is a password manager?

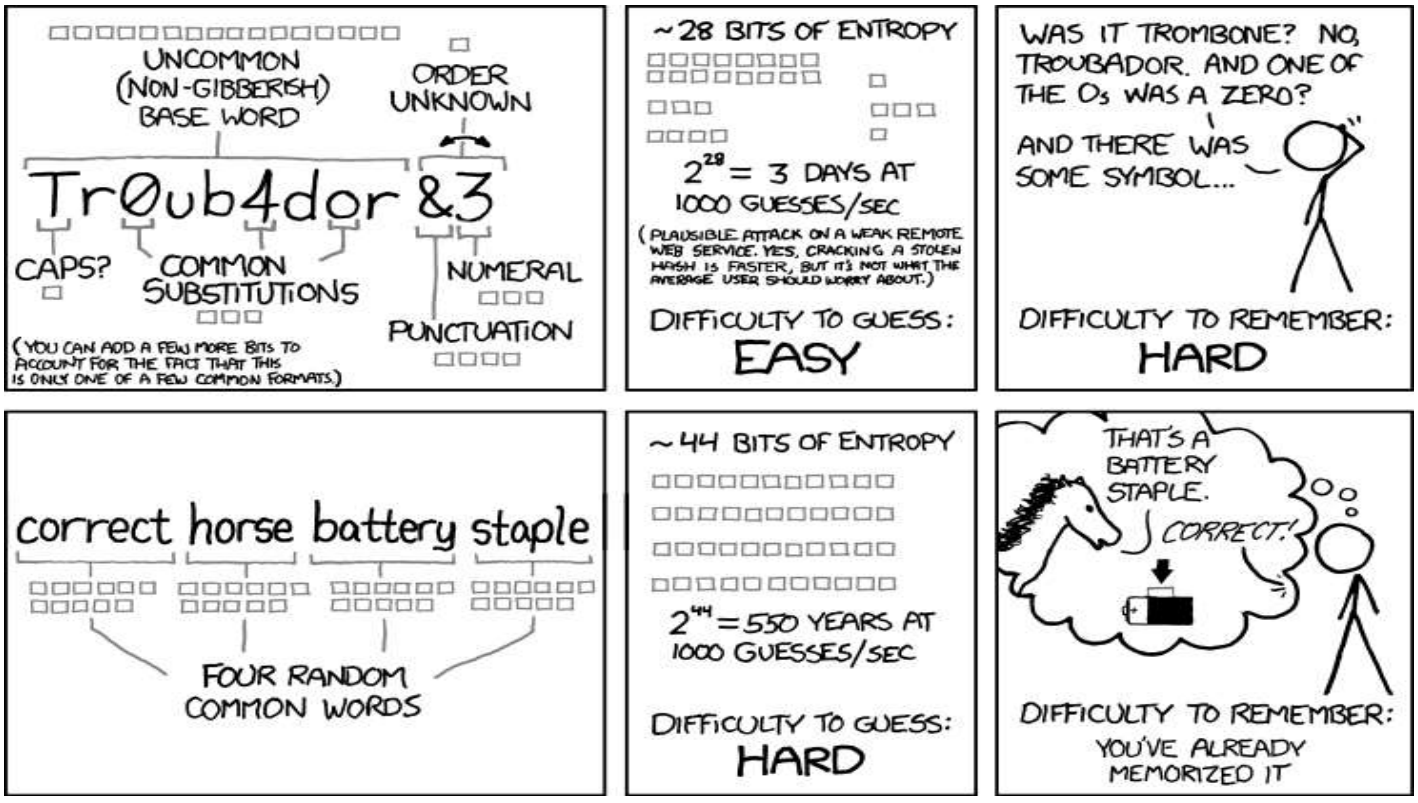
Malwarebytes

Once upon a time, during the early years of the Internet, you may have had a handful of passwords for a few essential web applications that you used to shop, study, stay connected, and get work done. Today, things are much more complicated. A 2017 report from LastPass found, on average, people had to remember, in some cases, hundreds of different passwords, just for work, not to mention their personal passwords.

While technology promises to make our lives easier, and it generally does, every new website and application we sign up for is another password we have to remember. For most, it's become impossible to remember all of them. The 2019 Google Online Security Survey found 52 percent of respondents reused the same password for multiple (but not all) accounts. This is a big no-no. Using giant lists of stolen passwords (aka "dumps") bought off the dark web, cybercriminals can brute force their way into other sites or use old passwords to extort users in scams. This is the data breach domino effect. One breach leads to another and another and so on.

According to the 2019 Verizon Data Breach Investigations report, 80 percent of data breaches are caused by compromised, weak, and reused passwords.

So, how did we get here, and what can we do about it?



The famous **xkcd** web comic "Password Strength" explained it best: "Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess."

It's true. 20 years ago cybersecurity professionals admonished consumers for failing to change default passwords on IoT devices (like your Internet router) or using easy to guess passwords like "12345" or "password". Out of this came the long and strong password **xkcd** pokes fun at, ie: *a common word with a mixture of uppercase and lowercase letters, at least one number, and one symbol.*

When creating a new account, websites demand that we create long and strong passwords. Failing that, we aren't even allowed to make an account. Assuming one gets past the account creation phase, you're going to promptly forget the Enigma machine cypher you just made and resign yourself to using the "Forgot Password?" link as your everyday log in option. Fortunately, you don't have to remember all those passwords. A password manager can remember them for you.

Malwarebytes Labs defines a password manager as "a software application designed to store and manage online credentials. It also generates passwords. Usually, these passwords are stored in an encrypted database and locked behind a master password." Once all your account usernames and passwords have been entered into the vault, your master password is the only one you have to commit to memory. Entering your master password unlocks your password vault, and from your vault you can then retrieve whatever password you need.

What are the benefits of using a password manager?

You don't have to memorize all your passwords anymore. You only need to remember the master password that unlocks your password vault and if you opt for a cloud-based password manager, you can access your password vault anywhere, from any device. These managers can auto-generate highly secure passwords for you. Password managers will typically ask you if you'd like to use an auto-generated password whenever you create a new account with a website or application. These random passwords are long, alphanumeric, and essentially impossible to guess.

They can alert you to a phishing site. Spam emails are spoofed or faked to look like they're coming from a legitimate sender, like a friend, family member, co-worker, or organization you do business with. Links contained within the email direct you to similarly spoofed malicious websites designed to harvest login credentials. If you're using a browser-based password manager, it will not auto-complete the username and password fields since it doesn't recognize the website as the one tied to the password.

Password managers save time. Beyond just storing passwords for you, many password managers also auto-fill credentials for faster access to online accounts. In addition, some can store and auto-fill name, address, email, phone number, and credit card info. This can be a huge timesaver when shopping online.

Many password managers help protect your identity. In a roundabout way, passwords managers help protect against identity theft, and here's why. By using a unique password for every site, you're essentially segmenting your data across each website and application you use. If a criminal hacks one of your accounts, they won't necessarily be able to get into any of the others. It's not foolproof, but it's an additional layer of security that you'll certainly appreciate in the aftermath of a data breach.

Are password managers safe?

Password managers have been hacked, but their overall track record when it comes to securing user data is very good. Password manager LastPass suffered a data breach in 2015. During the breach, cybercriminals made off with user emails but did not manage to steal any passwords. Even if they did, most password managers, including LastPass, use hardcore military-grade encryption to keep passwords safe.

Compare this to Facebook, Google, and Twitter. Going back several years, all three tech giants have admitted to accidentally storing passwords, for some of their users, in plain, readable text, no encryption to speak of and in the case of Google, all the way back to 2005. As far as anyone knows, none of the passwords were stolen, though Google reset affected passwords "out of an abundance of caution" immediately after discovering their mistake.

What are the types of password managers?

1. Desktop-based password managers store your passwords locally on your device, like your laptop, in an encrypted vault. You can't access those passwords from any another device and if you lose the device, then you lose all the passwords stored there. Locally-installed password managers are a great option for people who just don't want their data stored on someone else's network. They strike a balance between privacy and convenience by allowing you to create multiple password vaults across your devices and sync them when you connect to the Internet.

2. Cloud-based password managers store your encrypted passwords on the service provider's network. The service provider is directly responsible for the security of your passwords. The primary benefit of cloud-based password managers, RoboForm, 1Password and LastPass being good examples, is that you can access your password vault from any device as long as you have an Internet connection. Web-based password managers can come in different forms, most commonly as a browser extension, desktop app, or mobile app.

3. Single sign-on (SSO). Unlike a password manager that stores unique passwords for every application you use, SSO allows you to use one password for every application. Think of SSO as your digital passport. When entering a foreign country, a passport tells the officials at customs and immigration that your country of citizenship vouches for you and that you should be allowed to enter with minimal hassle. Likewise, when using SSO to log into an application, you aren't required to verify your identity. Instead, the SSO provider vouches for your identity. Businesses favour SSOs over password managers for a few reasons. Chiefly, SSO is a secure and convenient way for employees to access the applications they need to get their jobs done. SSOs also reduce the amount of time IT spends troubleshooting and resetting forgotten passwords.

Password best practices.

Don't reuse passwords, even with a password manager. Instead, create unique passwords for every site and let your password manager do what it's designed to do.

Create complex passwords. Many password managers helpfully auto-suggest strong passwords whenever you create an account for a new site. If not, try to use a random combination of letters and numbers and shift between uppercase and lowercase. The more complex and nonsensical, the better, especially since you won't be required to remember it. The password manager will do that. The one key difference is in creating your master password (the one that unlocks all the other passwords). This one you will need to remember, so unless you've got an eidetic memory, try to think of something memorable to you, but not easily traced back to your identity. Then add in some caps, some letters, and some fancy characters, and you've got a well-protected password vault.

Use a passphrase. When it comes to creating your master password (the one that unlocks your other passwords), try using a passphrase; i.e., a series of words that are easy to remember, but hard to guess. Something familiar with a strange twist, for example: "The P76 was the best car ever made." Or just a bunch of random things that a human can easily visualize, but a computer can't: "fancy rat neon avocado car." Use your imagination! Pets, children, or other family names, or lines like "Let me in!" are far too common, and therefore easy for cybercriminals to decipher.

Enable two-factor (2FA) or multi-factor authentication (MFA). One of the best ways to secure any account, password manager or not, is to enable MFA. With an MFA-enabled password manager, you'll be required to verify your identity using two or more authentication factors, which include something you know, something you possess, and something you are. The something you know is typically your password, but it can also be a PIN number. Something you possess might be your mobile phone, bank card, or a security token on a USB stick. Finally, something you are can be verified using biometrics, such as facial, voice, or iris recognition and fingerprint ID.

This extra layer of security means anyone attempting to log into your account (yourself included) will need to control those additional authentication factors outside of username and password.

An example of this would be after entering your master password to access the password manager, a code would be sent to your mobile phone, which you would then need to enter before accessing the vault. One thing to keep in mind when using your phone as an authentication factor—phone numbers can be hijacked. It's called SIMjacking (aka SIM-swapping) and it happens when a cybercriminal, posing as you, convinces your phone carrier to reassign your phone number to their phone by successfully answering your security questions. A cursory social media search is often all it takes for crooks to glean the answers they need. And once criminals have control of your phone, they have everything they need to steal your identity. Accordingly, you might look to a software-based authenticator like Authy or Google Authenticator instead for critical accounts.

Think twice about free password managers. Many of the most popular free password managers actually operate under a freemium business model, meaning you have to pay up if you want the best, sometimes essential, features.

- Do you need your passwords to sync across browsers and devices?
- Do you need digital inheritance?
- Do you need to share logins with family?
- Do you need multi-factor authentication?

Free password managers don't usually include these features. MFA, in particular, is a must have. In the debate between free vs. paid, opt for a paid password manager.

Create a password manager policy. Here's a tip for small and medium-sized businesses: Create a password manager policy and let employees know it's okay to use a password manager to secure their work accounts. Your staff are already using a hodgepodge of potentially insecure methods to try and manage their many passwords, and most data breaches start with a weak or reused password.

RoboForm is a good one, it can be configured to operate solely on one compute or can be cloud based whereby one password will open it and unlock programs on your desktop, your laptop and/or your phone, and you can mix things up too, you can have a PC desktop, an iPad and either an iPhone or Samsung phone and it will work.

An official password manager policy is your first line of defence against a cyberattack on your network.

Facebook Warning.

"If someone named "Bill Smith" (or some other name) wants you to add them to your account, don't accept – it is a virus. Tell everybody, because if somebody on your list adds them, you get

*the virus too. **copy and paste and please re post* this has been confirmed by Facebook and Snopes."*

Or

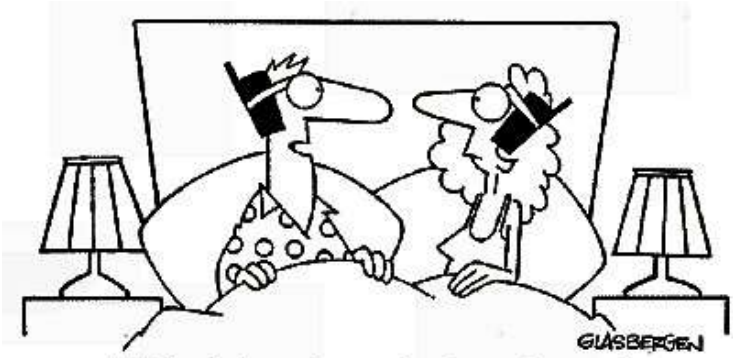
Please tell all the contacts in your messenger list not to accept a friendship request from Bill Smith. He is a hacker and has the system connected to your Facebook account. If one of your contacts accepts it, you will also be hacked, so make sure that all your friends know it. Thanks. Forwarded as received. Hold your finger down on the message. At the bottom in the it will say forward. Hit that then click on the names of those in your list and it will send to them

The examples reproduced above are nothing but a long-running hoax which warn readers not to allow contact from a particular person or group because dire consequences will result. Variants of these messages are circulated endlessly, with different names swapped in and out as various pranksters decide to play jokes on people they know by inserting their acquaintances' names and addresses into the warning in place of the existing information.

The most common variant of this hoax is one that warns the reader not to accept Facebook friend requests from "hackers" purportedly named "Christopher Davies" and "Jessica Davies," otherwise one of the two will wreak some unspecified havoc by being able to "FIGURE OUT YOUR COMPUTER'S ID AND ADDRESS." (The latest version also incorporates a hoax warning about the non-existent "Dance of the Pope" cell phone virus.)

Of course, it's not outside the realm of possibility that an e-mail message or a link posted on Facebook might carry a virus payload which could infect your computer and allow it be controlled by a botnet, but virus warnings that correspond to the patterns detailed above can be safely dismissed as japes.

See what Snopes has to say HERE.



"With wireless sleep technology, the people in my dreams can send e-mail and faxes to the people in your dreams!"

O

This page left blank