Technology Training Group

1300 13 66 79

easyLEARN Newsletter

!!!WARNING!!!

Facebook is planning to start scanning your brain for private information through your computer monitor. To stop this from happening, go to Kitchen –> Cabinets –> Upper Right Drawer –> then REMOVE the box that says 'Aluminum Foil'.

Then wrap all foil around your head.

Share this to warn all your friends!

Nov 2016

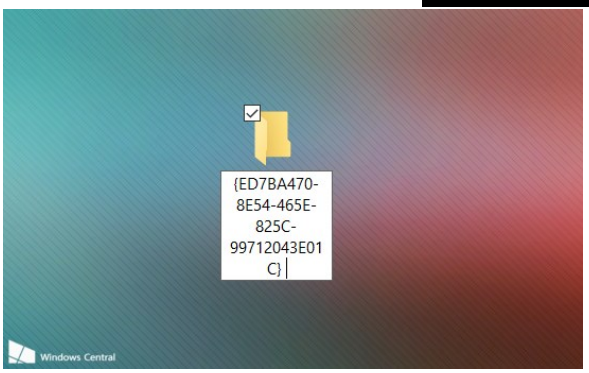
In this issue:

- ***How to enable "God Mode" in Windows 10***
- ***How to avoid falling victim to a phishing scam***

If you are a long-time Windows user, you may remember a trick to enable 'God Mode'. It may sound epic depending on your expectations, but the easiest way to describe the feature is that it gives access to *all of the operating system's control panels from within a single folder*. In fact, its real name is the *Windows Master Control Panel shortcut*. *God Mode* was an inside joke, but one that stuck.

As it turns out, you can enable God Mode in Windows 10 as well. Why would you need it? The feature is useful for those in IT, those who manage a computer, and obviously for those advanced enthusiasts. Most consumers have little need for the feature, and in fact, it could lend itself to doing some damage to the OS.

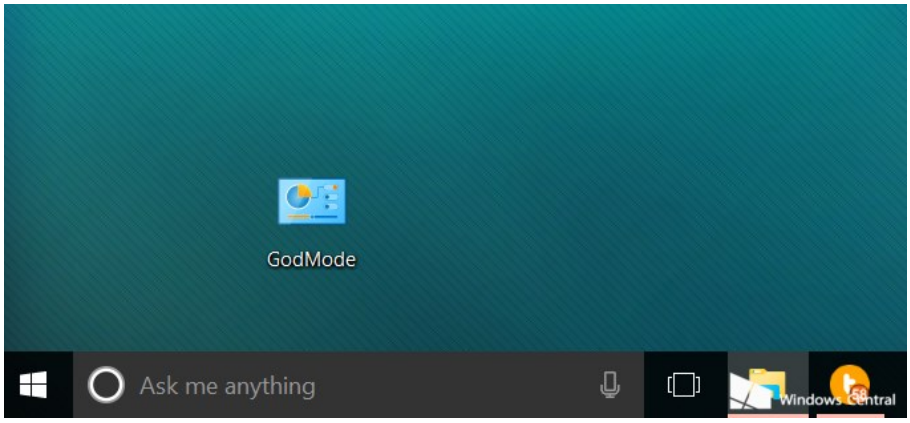
Think of God Mode as a backdoor to the OS to access all the settings. Of course, just enabling it does nothing, but just don't tinker around too much without an OS backup. So let's get to it:



Enable God Mode in Windows 10.

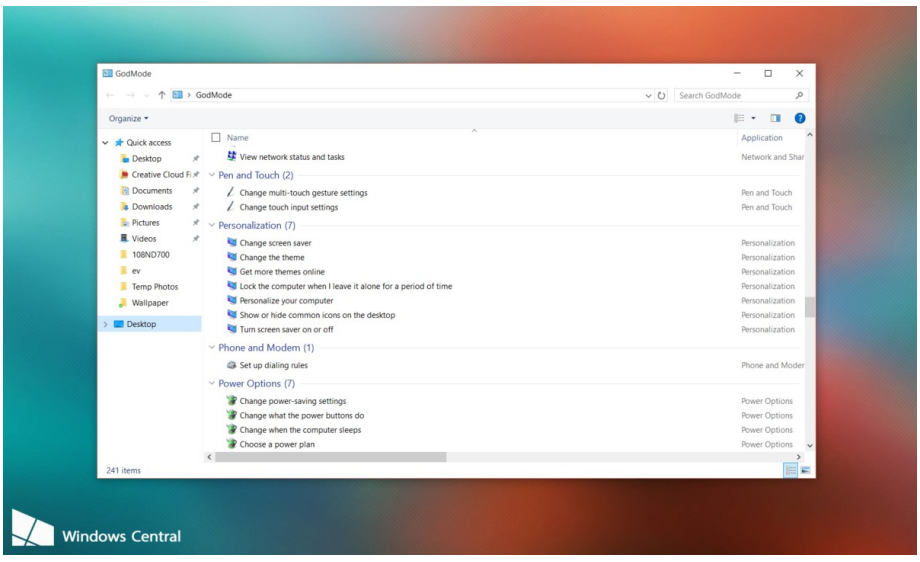
1. Make sure your system account has administrative privileges
2. Right-click on the Windows 10 desktop and choose **New** > **Folder**

Name the folder: **GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}** and hit **enter/return** to make it stick.



You can actually name the folder anything you want like **NinjaCat mode**. Simply replace 'GodMode' before the {….} characters to your liking.

That's it. Now when you open that folder, you can see around 40 different settings, including *Devices and Printers, Credential Manager, Indexing*, etc. Some variations exist depending if you have a Home or Pro version and different hardware.

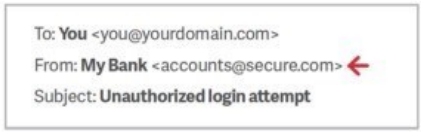


How to **Avoid Falling Victim To An Email Phishing**

One of the most popular ways for cybercriminals to steal personal information is by using email phishing scams. Cybercriminals often use this method of attack to trick employees from large organisations into clicking onto malicious links so they can gain access to corporate networks that contain valuable data. Here are 10 tips on how to avoid becoming a email phishing victim. Phishing emails often masquerade as correspondence from a legitimate and trusted organisation, luring victims to click on links that will make them download malicious content or trick them into inputting sensitive information onto a fake website.

Don't Trust The Display Name

A favourite phishing tactic among cybercriminals is to spoof the display name of an email. Here's how it works: If a fraudster wanted to impersonate the hypothetical brand "My Bank", the email may look something like:



Since My Bank doesn't own the domain "secure.com", email authentication defenses will not block this email on My Bank's behalf.
Once delivered, the email appears legitimate because most user inboxes and mobile phones will only present the display name. Always check the email address in the header from — if looks suspicious, flag the email. It's important to note that email addresses can be faked so it's not a fool-proof indicator.

Look But Don't Click

Cybercriminals love to embed malicious links in legitimate-sounding copy. Hover your mouse over any links you find embedded in the body of your email. If the link address looks weird, don't click on it. If you have any reservations about the link, delete it.

Check for spelling mistakes

Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

Analyse The Salutation

Is the email addressed to a vague 'Valued Customer?' If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

Don't Give Up Personal Or Company Confidential Information

Most companies will never ask for personal credentials via email — especially banks. Likewise most companies will have policies in place preventing external communications of business IP. Stop yourself before revealing any confidential information over email.

Beware Of Urgent Or Threatening Language In The Subject Line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or ask you to action an "urgent payment request."

Review The Signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details. Check for them.

Don't Click On Attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

Don't Trust The Header From Email Address

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address, including the domain name. Keep in mind that just because the sender's email address looks legitimate (e.g sender-name@yourcompany.com), it may not be. A familiar name in your inbox isn't always who you think it is.

Don't Believe Everything You See

Phishers are extremely good at what they do. Many malicious emails include convincing brand logos, language, and a seemingly valid email address. Be skeptical when it comes to your email messages — if it looks even remotely suspicious, do not open it.

For more information visit www.scamwatch.gov.au or click here. If you fear you have been a victim of a scam or are unsure about anything, feel free to contact me anytime for free advice.