Keep Your PC and Private Details Safe from the Dangers of the Internet

This article shows you how to:

✓ Ensure your PC is protected from online threats

✓ Understand the tricks criminals use on the Internet

✓ Avoid falling victim to the latest scams

Flick through any newspaper these days and you'll come across all sorts of headlines about hacking attacks, people being tricked, spyware threats, and much more. All this might well make you wonder where the real dangers lie for ordinary PC users. In this article, I'll explain the most important things you need to know when it comes to your PC's security.

Make Sure You're Aware of the Risks!

The main threat: Internet use

Ask a thousand experts about the specific dangers of using a PC and you'll probably receive hundreds of different answers. Effectively, though, those dangers will all boil down to just one: the Internet.

It's a vital area of computing…

Most of our PCs are connected to the Internet these days, and if they weren't, computing wouldn't be remotely as useful or enjoyable as it is. The Internet is rich with entertainment, information, advice and help, as well as offering many convenient ways to do your shopping and communicate with family and friends.

…but also a risk

Unfortunately, criminals know all about the Internet too, and it's as important to their activities as it is to ours. It allows them to operate anonymously from anywhere in the world, pretend to be someone they're not, and target millions of people at once rather than having to select one individual at a time.

Of course, this means that criminals use a scattergun approach, laying traps and seeing who falls into them. One obvious way of avoiding these traps is never to connect your PC to the Internet, but that's rather like suggesting you never walk anywhere in case you trip over.

The primary threats and their solutions

A more practical solution is to make sure you know exactly what the risks are and what you should do to counter them. Over the following pages I'll explain all the main dangers and the steps you should take to protect yourself from them.

Basic Security: Keep Your Software Updated

Security methods evolve constantly

Centuries ago, houses didn't have doors. These days, not only have we filled that inviting-looking hole in the wall, but we keep the door closed and secure it with locks that have become ever-more difficult to bypass. As the risks grow, the security measures we use have to change and improve in response to them.

Regular software updates improve security

The threat: The same reasoning holds true for Windows and the other software on your PC. The only difference is that in the fast-moving world of computing, new security measures are added in days or weeks rather than years or decades. This is because online criminals are constantly on the lookout for weaknesses in your system – new ways to 'pick your PC's lock', so to speak – and there's an endless game of cat-and-mouse going on in which the software companies try to close any gaps in security before the criminals can take advantage of them.

Keep Windows updated

The solution: 'Closing the gaps' is what the regular updates for Windows and other programs aim to do. Each update boosts the level of security on your PC, at least for the time being: potential intruders who know about a particular security flaw in Windows won't be able to exploit that flaw on your PC once the appropriate update has been installed.

Here's how to make sure you're receiving these vital updates:

Windows 10

- In Windows 10, very sensibly, updates can't be switched off, so you're certain to be receiving them. However, you should check that other Microsoft software (such as Office) is also being updated. To do that, open the Settings app (by pressing ⊞ + I), click on **Update & Security** followed by **Advanced options**. Below the words **Give me updates for other Microsoft products when I update Windows**, make sure the switch is 'On'.

Windows 8.1 and 7

- In Windows 8.1 and 7, set the Windows Update feature to install all updates automatically. Start Windows Update from the Control Panel or Start menu and click

Change settings. In the 'Important updates' section, choose **Install updates automatically (recommended).** A little further down, ensure that **Recommended updates** and **Microsoft Update** (if shown) are also enabled.

Other programs

- Some of the programs you use, such as Mozilla Firefox and Adobe Acrobat Reader, have options to update themselves automatically, checking for newer versions each time you start them, and these should be switched on. In most cases you'll find update-related settings in the Options/Settings/Preferences dialog, or in the Help > About dialog.

Manual updates

- Other programs you use may include an option to check for updates, but one you have to use manually, often by clicking a **Check for Updates** item on a menu. It's worth doing this regularly in order to keep those programs as up-to-date as you can. Pay particular attention to programs that access the Internet (such as web browsers and email programs) and programs you use to open files you've downloaded (such as PDF readers and media players).

Install and Use Anti-malware Software

VIPs need extra security

Famous people have a difficult time protecting their privacy, and they usually enlist some extra help: a security company that can keep intruders at bay, install cameras and fences, and see off the paparazzi.

PCs need a helping hand too

The threat: We may be just ordinary folk, but our computers are all VIPs: criminals want to get their hands on our computers and data, whoever we are. And even if we follow all the rules about keeping our software updated, we need our own equivalent of a security firm to spot intruders and send them packing.

Use security software

The solution: Make sure you have a good security program which monitors activity on your PC every second it's switched on, and use a second security program to run regular weekly scans to ensure nothing managed to evade the defences of the first:

Something to keep constant watch

- **An 'always-on' security program:** Windows 10 and 8.1 users are covered in this department with a built-in program named Windows Defender. If you're using Windows 7, I recommend the free Microsoft Security Essentials which you can find at tinyurl.com/pcksMSE.

A second malware scanner

- **An 'on-demand' security scanner:** I recommend the free version of Malwarebytes for Windows, which you can download from malwarebytes.com. After installation, you'll initially be using a trial version which gives you real-time ('always-on') protection. The trial ends after 14 days, but that's fine: unless you choose to pay for Malwarebytes (and it is an excellent program), you can still use it to run regular scans of your PC, and that's really the intention.

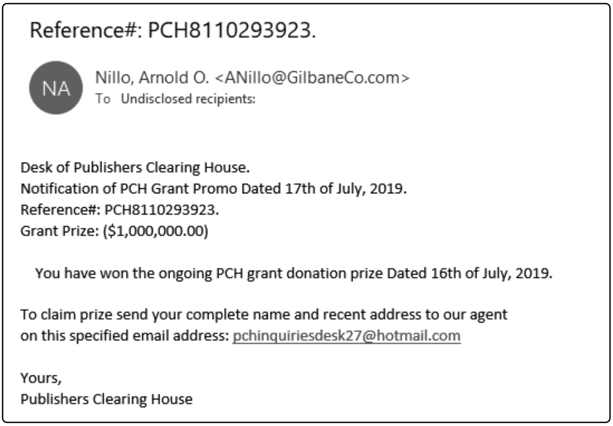
Email Threats: Dangerous Attachments and Phishing Scams

Scam emails are easy to send

We're as easy to contact by post as we are by email – our postal addresses are public knowledge, after all – but we rarely find anything more troublesome than a bit of junk mail on our doormats. That's because criminals can send vast numbers of email messages in next to no time, at little cost and no risk, and they use every trick they can think of to profit from it.

They prey on fear and greed

The threat: Email scams usually fall into two categories, targeting either fear or greed. Examples of 'fear' messages are those pretending that your bank has frozen your account, or that you've been billed for some expensive item from an online shop. Examples of 'greed' messages include a pretence that you're due a tax refund, or that you've won a lottery you've never heard of, or that a foreign bank official will slip a fortune in your pocket for helping him move funds out of the country.



Reference#: PCH8110293923.

NA Nillo, Arnold O. <ANillo@GilbaneCo.com>
To Undisclosed recipients:

Desk of Publishers Clearing House.
Notification of PCH Grant Promo Dated 17th of July, 2019.
Reference#: PCH8110293923.
Grant Prize: ($1,000,000.00)

You have won the ongoing PCH grant donation prize Dated 16th of July, 2019.

To claim prize send your complete name and recent address to our agent
on this specified email address: pchinquiriesdesk27@hotmail.com

Yours,
Publishers Clearing House

Never do what you're told!

In every case, the real threat is that you believe the message and do what it asks – that you'll click the links it provides, open the file attached to it, or contact the email address or phone number given. The intention of the messages is that you'll provide personal and financial details, or pay an advance fee on the promise of receiving a much larger sum in return, or allow malicious software to be installed on your PC.

The solution: To avoid falling into these traps, approach any unusual message with caution, particularly if it suggests an unexpected windfall or a sudden urgent problem:

Good fortune

- Be sceptical of any message that seems too good to be true. How could you possibly win a lottery without entering it? Is a rich philanthropist really likely to give you – a random stranger – money when there are so many more deserving causes? Would a foreign bank official tell you who he is and where he works, and then announce that he's planning to defraud his employer?

A sudden urgent problem

- Be just as sceptical about messages that seem designed to worry you and demand urgent attention. These will often be from someone posing as your bank, or HMRC (the old Inland Revenue), or an online store. Ask yourself whether the message looks as though it was sent to you personally, and only to you. If it really was, it would include your name and account number. Without these personal details, the same message could have been sent unchanged to thousands of other email users.

Always verify the sender

- Don't click links or open attachments in email messages if you're in the tiniest doubt about the message's authenticity. Instead, use your usual method to visit the website, or send an email, or pick up the phone. This way, you can be sure you're looking at the right website or talking to the right person, and you can then find out whether there's any truth to the message you've received.

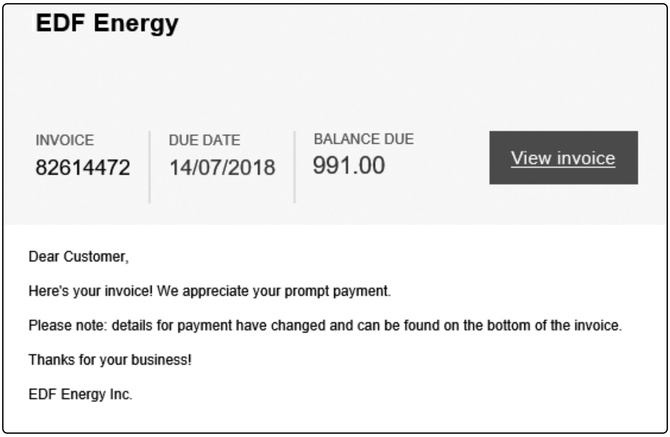
The Silent Menace: Drive-by Downloads

We can all have bad luck

How do you catch a cold? Well, you probably don't do anything wrong – you just happen to have stood in a supermarket queue or sat on a crowded bus, and that was all it took. And sometimes, too, your PC can catch its own kind of infection without your having done anything that was obviously 'wrong'.

A PC infection without your noticing

The threat: Online criminals would love to get their malicious software onto your PC, and one of the ways they do it is via websites. They may set up a clone of a well-known site which they fool you into visiting by email, or they may find a way to hack a legitimate website. You can find that simply by visiting the website, your PC becomes infected with the malware. This is known as a ‘drive-by download’, a reference to malware being downloaded and installed while you were ‘just passing’.



EDF Energy

INVOICE	DUE DATE	BALANCE DUE
82614472	14/07/2018	991.00

Dear Customer,

Here's your invoice! We appreciate your prompt payment.

Please note: details for payment have changed and can be found on the bottom of the invoice.

Thanks for your business!

EDF Energy Inc.

Software updates

A similar trick they use is to bundle malware with a tempting free program, to be silently installed on your PC at the same time as the main program.

The solution: There are several things you can do to avoid becoming the victim of a drive-by download:

Suspicious email

- Keep your web browser and your anti-malware program updated as these are your first line of defence against drive-by downloads.
- Never click links in email messages unless you’re certain you know who sent the message and that they wouldn’t be sending you to an unsafe website.

Take care with new software

- Only install software that’s been recommended by someone you trust, or that you’ve researched beforehand, especially if it’s free.

- Always download software from its maker's website. This way, you can be sure that criminals haven't had the chance to bundle malware into it.

Download from a trusted website

- When installing free software, check each step of the installation carefully and refuse any 'optional extras' you're offered along the way.

Avoid unwanted extras

- Never agree to install something just because a message on a web page tells you it's required.

The Phone Scam: Is Someone Really Monitoring Your PC?

Phone calls warning of problems?

Think back to your pre-Internet life: did anyone ever telephone you to say they'd detected a problem with your fridge, or they'd noticed your TV was faulty? Of course not – how could they possibly know?

Telephone scams are big business

The threat: As we've become more suspicious of email, scammers have turned to the telephone instead. It's a big business involving large call centres set up for the purpose. They call you up and claim to be from BT, or Microsoft, or something more vague like 'the technical support department'.

Claims that your PC is infected

Their story varies, but ultimately they want you to believe that they're somehow monitoring your PC and they've detected that it's infected with viruses. They usually threaten to cut off your Internet connection if you don't sort it out, and then helpfully explain that they can do this for you. They often want you to make a payment online for this, and then they direct you to install software that allows them to take remote control of your PC and 'fix the problem'. Once you've done this, they'll scour your files to look for personal and financial information and quite likely install spyware. People have had their identities stolen and bank accounts cleared out after falling for this scam.

The claims are ludicrous

The solution: It's absurdly simple: just remember that it's all utter nonsense! The scammer hopes to blind you with technical details and frighten you with threats of being disconnected, but what they're saying is all quite impossible. Is BT monitoring every broadband connection in the country? Is Microsoft watching the behaviour of 1.5 billion Windows PCs? Could anyone afford to pay the vast armies of staff required to provide this service? And if they did have this huge, expensive operation in place for our protection, wouldn't they be shouting about it from the rooftops?

Just hang up

Quite simply, the moment a caller tells you they're phoning about a problem with your computer or your Internet connection, you can be certain you're talking to a scammer. That's the point to hang up, and there's no need to be polite about it. Certainly don't let things get as far as your making payments or installing remote-access programs.

The Number 1 Online Rule: Be Suspicious!

Your PC seems safe

We're naturally suspicious of other people when their behaviour seems a little unusual, but when you're sitting at your PC with no-one else around, it's easy to feel that everything's safe and comfortable.

It's a false sense of security

The threat: When your PC is connected to the Internet, there are people around – millions of them – and some of them are up to no good. Online criminals know that our guard is dropped when we're sitting comfortably at our PC. They also know that many PC users feel their computer is smarter than they are, and will be more inclined to believe something that appears on a screen than something they're told by a stranger in the street. This is how email scams manage to defraud so many people of so much money.

Always be suspicious!

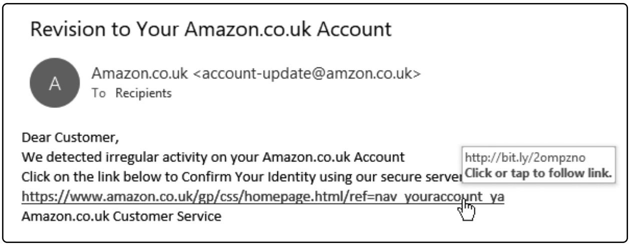
The solution: Where the Internet is concerned, a healthy dollop of suspicion is an absolute necessity. Although we've all seen many of the old scams many times and we recognise them instantly, there are new ones being dreamt up all the time. It's important to remember that things may not be quite what they seem:

Tall stories

- Remember that owning a computer doesn't make you any more likely to receive unexpected good fortune (lottery wins, tax refunds, cash windfalls), it just gives fraudsters an easy way to make you think that's what you're about to receive.

Disguised web links

- In an email message, don't assume the blue link that says (for example) 'www.amazon.co.uk' really will take you to 'www.amazon.co.uk'. Hold your mouse pointer over the link without clicking it and your email program should display a tooltip message beside the pointer (or at the bottom of the window) showing you the web address it really does lead to.



Revision to Your Amazon.co.uk Account

A

Amazon.co.uk <account-update@amzon.co.uk>
To Recipients

Dear Customer,
We detected irregular activity on your Amazon.co.uk Account
Click on the link below to Confirm Your Identity using our secure server
https://www.amazon.co.uk/gp/css/homepage.html/ref=nav_youraccount_ya
Amazon.co.uk Customer Service

http://bit.ly/2ompzno
Click or tap to follow link.

Research before installing

- If your casual web surfing leads you to a website offering a free program, don't assume the program is good – or safe – just because its maker says it is. Try searching for independent reviews and comments about it elsewhere.

Guilty until proven innocent

- In email, particularly, a wise approach is to start with the assumption that any unusual message you receive is a scam and then look for signs that it's legitimate: that the sender clearly knows who you are; that the message wasn't sent to other recipients at the same time; that the sender isn't trying to frighten you into taking hasty actions; and that the message isn't insisting you click a link or open an attachment to find out what's really going on.

The Obvious Precaution: Backup Your Files

If you fell victim to a malware attack that made your PC unusable, that might be very annoying. Indeed, it might cost you a little money to get it cleaned up and ready for use again. But there's something worse...

You could lose all your files

The threat: A malware attack could take away all your files – your documents, photos, and everything else. It might delete them, it might encrypt them and demand you pay a 'ransom' to regain access to them, or it might leave your system in such a mess that your files couldn't be recovered.

Keep regular backups

The solution: It's the obvious precaution, but many PC users find themselves wishing they'd done it when it's too late: backup your files!

Get into the habit of regularly taking safety copies of everything you wouldn't want to lose and couldn't possibly replace, keeping them on a high-capacity USB flash drive or memory card, or an external hard drive. Keep this drive disconnected from your PC when you're not actively backing-up files to it, so that if any disaster does befall the files on your hard drive, it can't take out your vital backup copies at the same time.