Guidance for safe computer and Internet use

Guidance Note C06/17

13th July 2017

Gibraltar Regulatory Authority
Communications Division
2nd Floor, Eurotowers 4,
1 Europort Road
Gibraltar
GX11 1AA
Telephone +350 20074636 Fax +350 20072166
Email: communications@gra.gi
Web: http://www.gra.gi

Guidance for safe computer and Internet use

Computers and the Internet have become a part of everyday life – from staying in touch with friends and family to sharing photographs, booking holidays and even doing your shopping online.

It's all really useful…if you know how. But, does the Internet open the doors to criminals?

In short, yes, it can do. The good news however, is that there are ways in which you can protect yourself from the threats they pose.

Q: So what are the threats and how can they affect me?

A: Threats are always changing depending on what criminals wish to gain, but generally, they're either after your money or your personal information and can now access these in more sophisticated ways that by rummaging through your drawers at home.

Q: Who could possibly want to do this to me and why?

A: Internet crime is as active today as it's ever been. The Internet has provided clever criminals with the ability to access people's homes and information without being physically present and worryingly they can now target thousands of homes/people in no time at all.

Q: But how is that possible?

A: Computers, mobile phones, laptops, tablets, gaming consoles etc……they all have one thing in common….they access the internet and often via a Wi-Fi connection. Skilled criminals can tap into (hack) your private Wi-Fi, observe your online activities and then access your online banking, personal passwords, online shopping and other transactions which you thought were perfectly safe.

Q: That's scary, what can I do to protect myself?

A: Much like you wouldn't carry a wad of cash in your hand on a busy street, there are some simple measures you can put in place to make yourself a less obvious target to scammers and hackers.

- **Staying safe when using the Internet.**

Discover how to keep you and your computer safe.

It is crucial that you recognise and delete suspicious online activity, create strong passwords for use on websites and learn how to shop safely on the Internet.

The Internet is a wonderful tool that has lots of benefits and can, in many ways, make your life better. Unfortunately, the features that make it easy for honest people to use can also be exploited by criminals and people intent in causing disruption. But you should not let fear stop you using the Internet. There are a few simple precautions that can keep you and your personal information safe.

- **Making sure your computer is secure**

It's important that your computer at home be protected from malware attacks which can sometimes infect your computer. Malware can be automatically installed when you connect an infected drive to your PC. Some other types of malware (called worms) can also spread by infecting PCs connected to the same network. Other types of malware are often sent as an email attachment which is designed to intentionally trick the recipient to open the infected file.

The good news is that you can protect your computer from the vast majority of malware attacks, by using special computer software such as; Firewall software, Anti-virus software and Anti-spyware software. There are free versions available to download that offer basic protection, but there are also far more advanced programmes available to purchase and offer higher levels of malware protection for your computer or device.

You can also find other tips for keeping your computer safe at www.getsafeonline.org

- **Network and device hacking**

Nowadays, you won't go too many days without hearing about the next big corporate "hacking" scandal and that the company's virtual security was cracked by hackers. It may also be no surprise to hear that corporations and established organisations are not the only ones getting hacked. Every so often we learn that ordinary people are also being hacked or have fallen victim to identity theft. Luckily though, there is a lot we can do to deter criminals from attempting to steal from us.

Start by securing your home network!

11 Ways to help Secure Your Wi-Fi Network

Before you decide to go and play around with your router’s settings, consider that if your router was supplied by your Internet Service Provider (ISP), you may have limited access to these settings and may require consent from your ISP before you can do so. If you bought the router yourself and are not tech-savvy enough to delve into the router settings, seek help from a reputable expert.

1: Change Your Router Admin Username and Password

The generic usernames are a matter of public record for just about every router in existence; not changing them makes it incredibly easy for someone who gets physical access to your router to mess with the settings.

2: Change the Network Name

It's usually a moot point if you have robust encryption in place, but just because you're paranoid doesn't mean they're not out to use your bandwidth. Remember, if you change the SSID and don't broadcast the SSID, it's on you to remember the new name all the time and reconnect ALL your devices—computers, phones, tablets, game consoles, talking robots, cameras, smart home devices, etc.

3: Activate Encryption

This is the ultimate Wi-Fi no-brainer; no router in the last 10 years has come without encryption. It's the single most important thing you must do to lock down your wireless network. Head to your router maker's support site or Internet Service Provider for guidance on how to do this.

4: Double Up on Firewalls

The router has a firewall built in that should protect your internal network against outside attacks. Activate it if it's not automatic.

5: Turn Off Guest Networks

If they're close enough to be on your Wi-Fi, they should be close enough to you that you'd give them the password.

6: Use a VPN

A virtual private network (VPN) connection creates a tunnel between your device and the Internet through a third-party server, which in some cases may limit the functionality of certain websites, depending on the VPN provider and the website being accessed. The VPN can help mask your identity or make it look like you're in another country, preventing intruders from seeing your Internet traffic. Some even block ads.

7: Update Router Firmware

Just like with your operating system and browsers and other software, people find security holes in routers all the time to exploit. When the router manufacturers know about these exploits, they plug the holes by issuing new software for the router, called firmware. Go into your router settings every month or so and do a quick check to see if you need an update, then run their upgrade. New firmware may also come with new features for the router, so it's a win-win.

8: Turn Off WPS

Wi-Fi Protected Setup, or WPS, is the function by which devices can be easily paired with the router even when encryption is turned on because you push a button on the router and the device in question. It's not that hard to crack and means anyone with quick physical access to your router can instantly pair their equipment with it.

9: Don't Broadcast the Network Name

This makes it harder, but not impossible, for friends and family to get on the Wi-Fi; that means it makes it a lot harder for non-friends to get online. Head to your router maker's support site for guidance on how to do this.

10: Disable DHCP

The Dynamic Host Control Configuration Protocol (DHCP) server in your router is what IP addresses are assigned to each device on the network. For example, if the router has an IP of 192.168.0.1, your router may have a DCHP range of 192.168.0.100 to 192.168.0.125—that's 26 possible IP addresses it would allow on the network. You can limit the range so (in theory) the DHCP wouldn't allow more than a certain number of devices — but with everything from home appliances to watches using Wi-Fi, that's hard to justify.

Do keep in mind that anyone with the right Wi-Fi hacking tools and a good guess on your router's IP address range can probably get on the network even if you do disable the DHCP server.

11: Filter on MAC Addresses

Every single device that connects to a network has a media access control (MAC) address that serves as a unique ID. Some with multiple network options — say 2.4 GHz Wi-Fi, and 5 GHz Wi-Fi, and Ethernet — will have a MAC address for each type. You can go into your router settings and physically type in the MAC address of only the devices you want to allow on the network. Head to your router maker's support site or Internet Service Provider for guidance on how to do this.

- **Email scams**

Be very careful when opening emails from unknown or suspicious sources. Every year, billions of pounds are extorted from the victims of scam emails around the world.

Remember that credible companies should NEVER ask you for your full passwords to them via email or on the phone. If you do encounter this, contact the company which you suspect is being impersonated and check that this contact is genuine. If it isn't, ensure the email sender is blocked and report it where possible.

5 tips to help you identify and deal with email scams

1: Is there urgency in the message?

A common tactic is to panic the "customer" causing them to respond so quickly that they haven't had time to think about what they are doing.

Sometimes the email will claim to be from a loved one in a state of distress and asking you for money. On other occasions you will be informed that an important payment has failed.

If you encounter this, don't open any accompanying attachments even if the email claims they are sending a receipt or some other additional information. The attachment could contain a file that, once opened, will install a virus on your device.

If the email is from a friend or family member asking you for money - it's possible that their account has been hacked by scammers. If you're really worried about them, trying getting in touch with them by phone first.

2: Thoroughly inspect the senders email address?

If an email is offering a deal that's too good to be true, then it probably is. Even if it appears to be from a legitimate business, friends or family members.

When emails claim to be from banks, online stores or other trusted organisations, check to see what the email address looks like. What's hidden underneath the sender name might be quite different from the name that you can see

Alarm bells should be ringing if the message has been sent from a free email provider, such as Gmail or Outlook.com, rather than associated with the company in question.

3: Who is the message addressed to?

If the email doesn't address you personally, but says something like 'Dear Customer' or 'Dear Friend', the message could well be part of a mass mail-out by scammers.

By sending out thousands of emails like this, criminals hope they can trick a few people into trusting them and unwittingly hand over their cash or personal information.

4: Are there links in the email?

If there are links in the email don't click on them even if they look genuine.

Just like the sender's details, they can appear to be harmless but the underlying web address can take you to the scammer's website.

This site might look identical to the one you'd expect to see but in fact be an imitation website.

If you enter payment details or other personal information this can be harvested and used for fraudulent purposes.

5: Is the message written in good English?

There are many small clues that can hint that an email is not trustworthy.

For example, a small difference in the company logo or the layout of the message looking sloppy and unprofessional. Check the spelling and grammar and be wary if there is an unusual use of capital letters in a sentence. If there's anything about an email that makes you feel slightly uneasy or nervous about an email you've received, just remember you don't need to respond immediately.

Take your time to work through these five steps whenever something makes you feel uneasy.

- **Password strength**

It may seem obvious, but the golden rule is to keep the password a secret and never write the password on a sticky note to keep on your computer screen, as this immediately takes the guess work out of the equation for those seeking to use it with malicious intentions.

Secondly and perhaps less obvious, is to never under any circumstances share your password over an email or over the phone to anyone you don't know personally.

Refrain from using your name, your children's names, your grandchildren's names or even your pet's names. Sometimes people use the name of an activity or company they are strongly associated with. This is information that hackers can easily get a hold of and eventually work out your password, particularly if your social media privacy setting are disabled.

If you'd like to check how strong your current passwords are, there are online password checkers if you search for them. If you're creating a new password, the website you are creating the password for will usually indicate the strength of the password.

Remember, use a word that you will remember, but one that may not be easy to guess. Always use a combination of numbers and letters in both lower and upper case to produce the strongest possible password in order to make it difficult for hackers and scammers to obtain it.

It is safer to have different passwords for different websites and email addresses and be sure to log off once you've finished.

- **Shopping on the Internet**

One of the benefits of the Internet is the ability to shop from a wide range of stores and buy items on auction sites. To protect yourself when shopping online follow these tips:

Use retailers that have a good reputation such as 'high street' shops, or established brands. Follow the security advice carefully on websites that you trust as it is there to help you. Never download illegal software, music or videos. Make sure that you are on a **secure site** when you need to give credit or debit card details. There will often be a padlock symbol either next to the address or at the bottom right corner of the page.

You can search on your preferred web browser for more information on what a secure site is and what else to look out for. Just type "what is a secure site" and hit search.

Jargon Buster

Address Book

Part of your email software where you store details of your ‘friends and contacts’ email addresses so you don’t have to remember them!

Anti-virus

Anti-virus software helps protect your computer from viruses.

Application

Another word for computer program. For example, Word, which is used for creating documents is a word processing application.

Archive

The place on a website where you find old articles, stories etc.

Attachment

A file which is ‘attached’ and sent with a standard text email message. Often photographs or Word documents are attached to emails.

Backup

A technical term for copying files onto disk or CD-ROM for safe keeping so that they are kept in more than one place.

Bcc

Means Blind carbon copy. The Bcc box allows you to send an email to more than one person but their email addresses are hidden from other recipients.

Broadband

A permanent high-speed Internet connection. It receives digital information at about 100 times faster than a dial-up modem and is “always-on”.

Browser

A program you use to view web pages and ‘browse’ websites. Google Chrome, Internet Explorer and Mozilla Firefox are some of the most popular browsers.

Bugs

Errors in a piece of software or web page that can make it break or work strangely.

Cc

Typing an email address or string of email addresses in the 'Cc' box will send your mail to those additional addresses as well as the main recipient.

Crash

When your computer temporarily stops working. It may pause or 'freeze' up, or tell you to restart or quit.

Cursor

The flashing vertical line on the screen that shows you where you are and where the next character you type will appear.

Cut and paste

Selecting text, images or files and deleting them from one place while putting them in another

Digital Cameras

A camera that takes photographs and stores them on disks or smart cards rather than on film. The photos can then be downloaded onto a computer where the images can be printed, put on a web page or emailed.

Driver

Software which runs hardware attached to your computer like a modem, printer or scanner. New hardware normally comes with a CD containing the necessary drivers to install on your computer.

Download

Getting a file onto your computer from another computer on the Internet. Drag and drop Clicking on an icon or selection, holding the mouse button down and moving the mouse to 'drag' the selection to a new location. When the mouse button is released the item is 'dropped'.

Email

Electronic mail. Messages (sometimes with attachments) sent over the Internet from one email address to another.

Error message

A 'complaint' by the computer that something has gone wrong, maybe including an 'error code'.

FAQ

Frequently Asked Questions. A list of standard answers to questions which newcomers to a topic or website may have.

File

Data stored on a disk. There are two types: 'program files' (with instructions that make up software applications, e.g. Word) and 'data files' (files created by you and me, e.g. a letter or photo).

Firewall

A program which sits between your computer and the Internet and watches for hacking, viruses or unapproved data transfer.

Flash

A plug-in application you download which allows your browser to show animations.

Hacking

Unauthorised access to a computer, its files and programs by a 'hacker', a computer expert who can break through its security.

Hard drive/Hard disk

The place inside your computer where you save documents, pictures, applications, etc.

Homepage

The 'front page' of a website, where you're told what's on the site, how to get around it and how to search for things that'll interest you.

Hypertext

Text which is arranged in a non-linear fashion and which you continue reading by clicking on links.

Icon

A small picture which, when you click on it launches an application, program or acts like a link on the World Wide Web.

Inbox

The folder in your email program/webmail where you get your incoming emails.

Internet

Millions of computers around the world connected together by telephone lines, cables or satellites.

Internet Explorer

One of the most popular web browsers, designed by Microsoft.

ISP

Internet Service Provider. An ISP is the company that provides Internet connections.

Junk email

Direct marketing sent by email rather than by the post.

Laptop

A small, portable computer which can be battery operated as well as run from the mains.

Link

Words or pictures you can click on which take you from somewhere (an Internet page, an email message etc.) to somewhere else (another page, a picture etc.).

Logging in

Using a username and password to prove your identity so that you can enter your computer or Internet account.

Macintosh/Mac

A family of computers developed by Apple.

Mailbox

The folder which contains a person's individual items such as an inbox, outbox, sent items, notes and calendar.

Malware

Types of malicious software that can infect computers and devices. The word malware is a combination of two words "malicious" and "software".

Memory

The storage and thinking parts of your computer. More storage memory on your hard disk (ROM) means you can save more files and more thinking memory (RAM) means your computer can perform more complex tasks quicker.

Monitor

The display screen on your computer.

Offline

Describes when your computer is not connected to the Internet.

Online

Describes when your computer is connected to the Internet.

Password

A series of letters, numbers and characters that you enter to get into your computer, Internet connection, email or websites that you are registered with.

Refresh/Reload

The button that you use to download a web page again. In Internet Explorer it's called "Refresh" and in Mozilla Firefox "Reload". You should press this button if for some reason a web page appears not to have loaded correctly.

Register

Some websites ask you to give your name, email address and other personal information in order to view pages. This is called registering.

Search engine

A search engine is usually a website which allows you to search the Internet for information. The search engine lists results that relate to your key words.

Software

Any programs such as word processors, email applications or Internet browsers.

SPAM

Junk email sent to many people at once, usually involving advertising or offering services. SPAM is very deeply frowned upon by most Internet users, and where it involves advertising or a false return address it is particularly disliked.

URL

Stands for Uniform Resource Locator, the technical term for the address of a website or document on the web (e.g. www.gra.gi).

Username

A series of letters and numbers you type into your computer, email account or other computer network service to tell it who you are.

Virus

Pieces of code that are designed to reproduce and damage data or system performance. There are thousands of viruses and the numbers keep growing.

Web browser

Software which allows you to surf the Internet.