iweb solutions
E-Business Consultancy

Online Safety Tips

Avoid Cyber Attacks:

- **Keep Personal Information Professional and Limited**

Potential employers or customers don't need to know your personal relationship status or your home address. They do need to know about your expertise and professional background, and how to get in touch with you. You wouldn't hand purely personal information out to strangers individually—don't hand it out to millions of people online.

- **Keep Your Privacy Settings On**

- Marketers love to know all about you, and so do hackers. Both can learn a lot from your browsing and social media usage. But you can take charge of your information. As noted by iWeb Solutions, both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook also has privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

○ **Practice Safe Browsing**

- You wouldn't choose to walk through a dangerous neighborhood—don't visit dangerous neighborhoods online. Cybercriminals use lurid content as bait. They know people are sometimes tempted by dubious content and may let their guard down when searching for it. The Internet's demimonde is filled with hard-to-see pitfalls, where one careless click could expose personal data or infect your device with malware. By resisting the urge, you don't even give the hackers a chance

○ **Make Sure Your Internet Connection is Secure.**

- Free wi-fi for an example.

  When you go online in a public place, for example by using a public Wi-Fi connection, you have no direct control over its security. Corporate cybersecurity experts worry about "endpoints"—the places where a private network connects to the outside world. Your vulnerable endpoint is your local Internet connection. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network) before providing information such as your bank account number.

- ◦ **Be Careful What You Download**
- A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather.

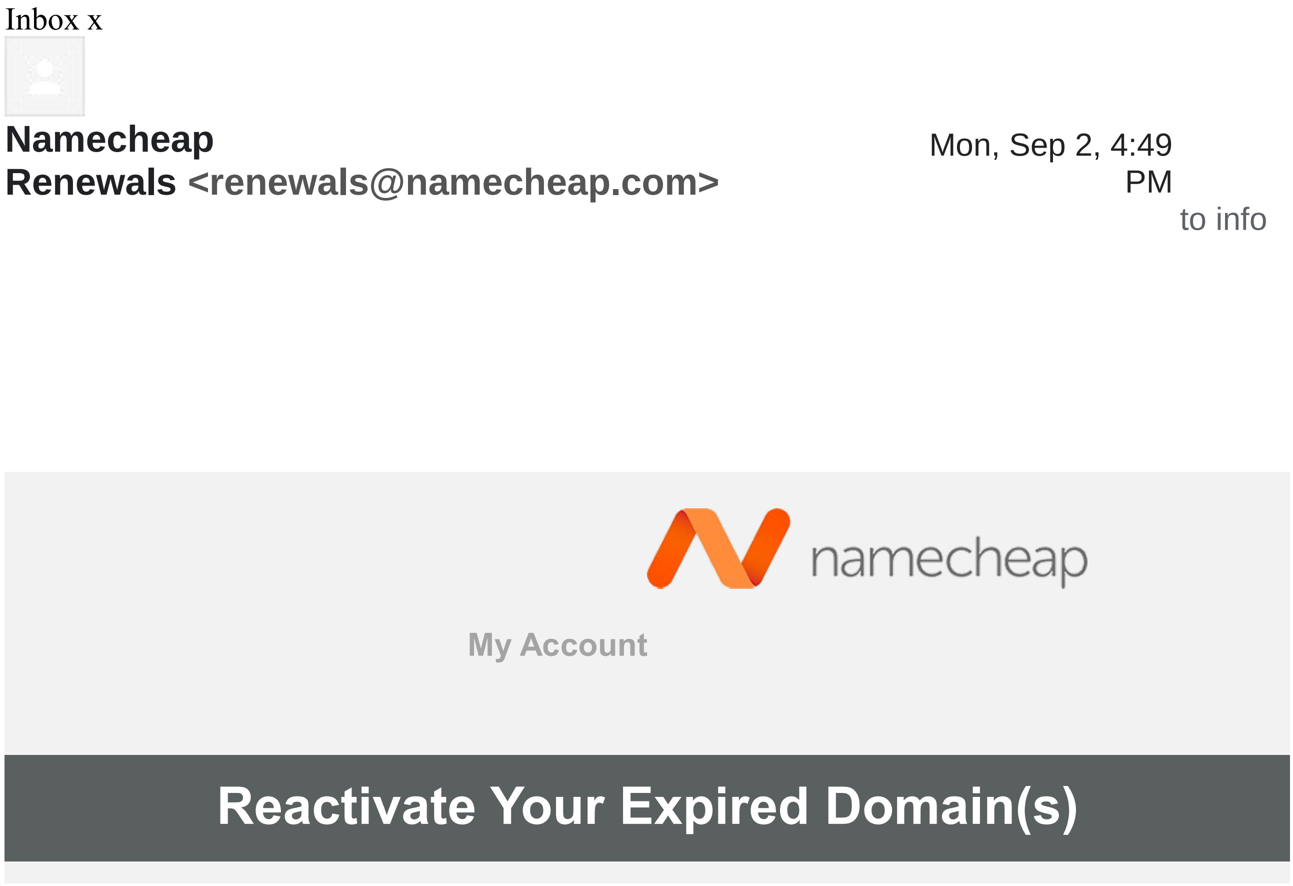
- ◦ **Choose Strong Passwords**
- Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters.

- ◦ **Make Online Purchases From Secure Sites**
- Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. As iWeb Solution advises, you can identify secure sites by looking for an

address that starts with *https:* (the S stands for *secure*) rather than simply *http:* They may also be marked by a padlock icon next to the address bar.

  - **Keep Your Antivirus Program Up To Date**

- Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.
- **Your Domain has expired**
  - Pat, yourdomain(s) have expired click here to renew. Do not click until you are 100% sure!



Namecheap Renewals <renewals@namecheap.com>

Mon, Sep 2, 4:49 PM

to info

Reactivate Your Expired Domain(s)

-

- Always check the source.
- Think first ask yourself did I apply for that,did I enter that draw?
- Always look at the web address in the top bar to see where this email is coming from
- Don't be fooled by the title ,because that is where you will get caught out.
- There was money left to you from a relative,would you not be notified by post or phone first? **Think about it!**