EzeCastle INTEGRATION

IT Security DOs & DON'Ts

Be Cyber Aware

TABLE OF CONTENTS

1. Do...

Be smart when browsing/surfing the internet or clicking links.

Hackers are skilled at creating fake professional looking websites so be on the look out for these signs that could signal it is a malicious site:

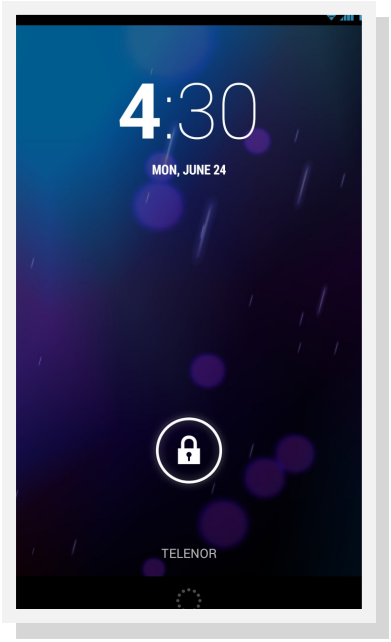
- Check for presence of an address, phone number and/or email contact
- Check the web address for misspellings, extra words, characters or numbers that seem off or suspicious
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser
- If there is NO padlock in the browser window or 'https://' at the beginning of the web address to signify that it is using a secure link, do not enter personal information on the site
- Be wary of websites that request lots of personal information
- Avoid 'pharming' by checking the address in your browser's address bar after you arrive at a website to make sure it matches the address you typed
- Be wary of websites that are advertised in unsolicited emails from strangers

Tips Source: *Get Safe Online (Nonprofit Organization)*

2. Do...

Lock your computer and mobile phone (s) when you leave your desk and/or office.

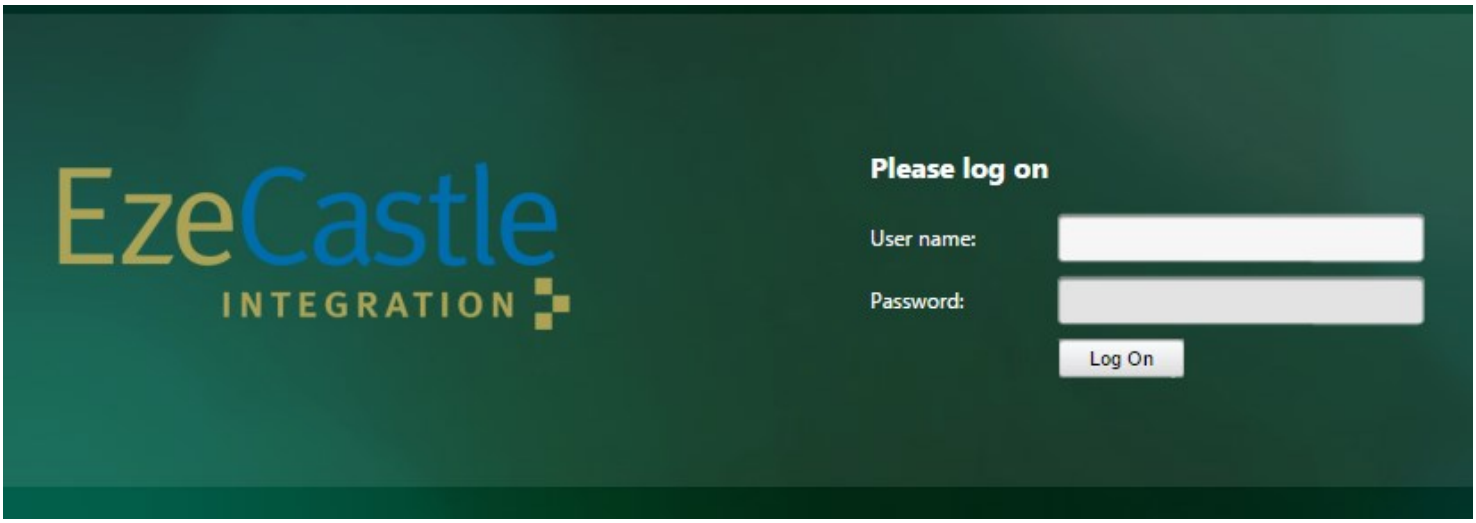
We recommend this to prevent unauthorized users from gaining access to your computer's hard disk and critical business data. To get in the habit of locking your devices, place a reminder note on your desk (e.g. next to keyboard).



3. Do...

Use care when entering passwords in front of others.

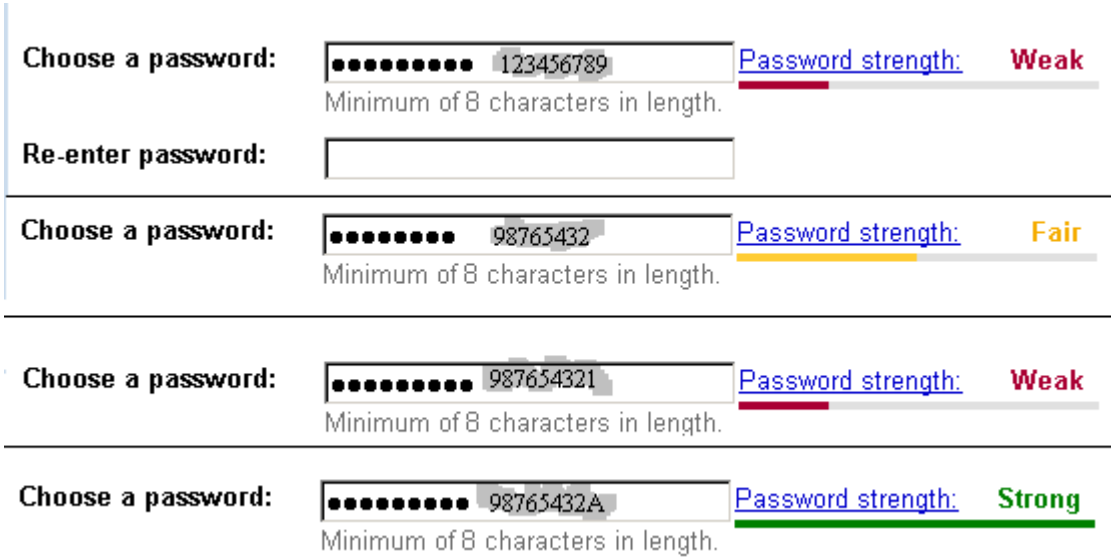
You can make login fields more secure by masking your password rather than having credentials displayed. Also, this one's obvious, but don't write your passwords down somewhere where they can be easily found by others. Employee awareness is critical, especially for protecting accounts belonging to the company.



4. Do...

CREATE AND MAINTAIN STRONG PASSWORDS AND CHANGE THEM EVERY 60-90 DAYS.

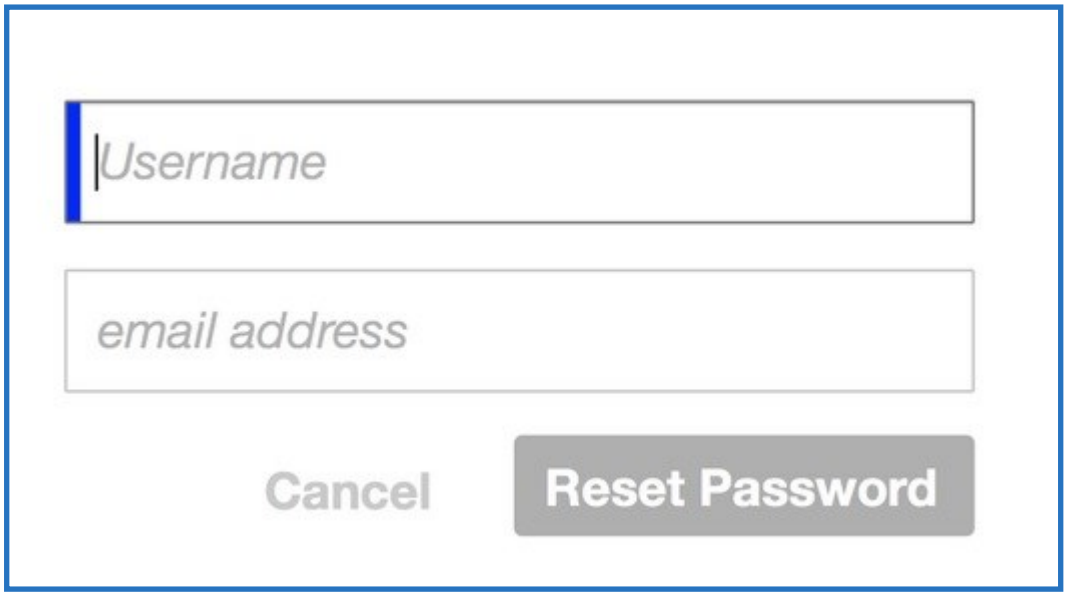
Simple passwords, such as “12345” or “abcde”, can be easily guessed. We recommend using a combination of upper and lowercase letters, numbers and special characters. We also recommend avoiding passwords with personal references that could be easily guessed (i.e. names, birthdays, kids’ names, etc).



5. Do...

CHANGE YOUR PASSWORD IMMEDIATELY IF YOU SUSPECT THAT IT HAS BEEN COMPROMISED.

Prevention is key. We highly recommend acting quickly even if you have the slightest hint that your password has been compromised. As always, be sure to use a strong password.



6. Do...

Protect personal computers and devices with anti-virus/anti-malware software when working remotely and keep it current.

It is expected that your office IT systems are protected with current anti-virus/malware software. However, security for your devices shouldn't end at your office doors. In today's world where telecommuting is becoming the new norm, it's imperative to take security precautions at home too. We suggest installing anti-virus/ anti-malware software and updating it regularly on your personal computers so that your data is safe no matter where you are.

7. Do...

Report suspicious activity to the IT team/CSIRT to help minimize cyber risks.

Waiting to report suspicious activity heightens threats and increases your chances of becoming the victim of hacking, system failure or data loss/destruction. Contact your IT team or Computer Security Incident Response Team (CSIRT) immediately to minimize risks.

8. Do…

Get rid of "Junk"

Old photos, videos, and archives only take up disk space and slow performance.

9. Do...

Check up on unused software

See what your programs are actually doing. If nothing, uninstall. This will reduce potential mal-ware targeted software.

10. Do...

Back up.

Store copies of your files on an external drive in case of a virus, the loss of a computer or smart device, or a hardware breakdown.

11. Do...

REVIEW SOCIAL SETTINGS

Make sure your privacy settings are what you intend them to be. Purge your “friend” list and contacts, being mindful of inactive profiles and contacts that are no longer relevant.

1. Do Not…

Open email or attachments if the sender is unknown or suspicious.

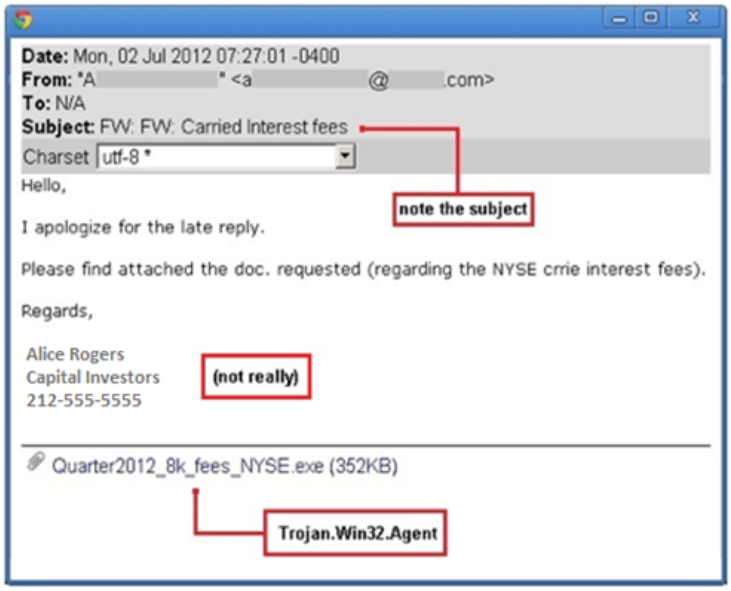
In addition, do not forward emails that you suspect are spam. Often, hoax emails, such as those containing instructions on how to prevent viruses, request that you delete important files. If you receive an email you aren't sure is legitimate, contact your IT department.

2. Do Not…

Get caught by phishing attempts, which can occur via email, phone, instant message, SMS or social media.

Phishing is a psychological attack used to trick you into giving up personal information or taking action. Signs to look out for include:

- Check the sender email address as well as "TO" and "CC" fields
- Is it personalized? Be wary of generic greetings
- Improper spelling and grammar can be giveaways as well
- An overwhelming sense of urgency requesting personal information
- Links! Only click on those that you are expecting (same goes for Attachments)
- Suspicious emails from trusted sources can happen. If your friend/colleague sends a strange message, their account may have been attacked.



3. Do Not…

Install unauthorized programs on your work (or home) computer.

We suggest only downloading authorized programs and plug-ins from known, reputable sources to protect your information and network. Malware can make its way into machines from downloads.

Use caution at home too as many "free" programs downloaded from the web install software that can track your behavior and show unwanted advertisements.

4. Do Not…

Provide information such as login IDs, passwords, social security numbers, account numbers, etc. via unencrypted email.

Email is not a secure means of transmitting confidential information. If you do not encrypt your device and emails, other users on your network and outside can easily capture your login credentials and messages you send or receive. This threat increases when utilizing a public network (e.g. an open Wi-Fi network or airport hotspot). When data is encrypted, it is unreadable and unusable by anyone lacking the proper tools to unlock the information.

5. Do Not…

Allow others to use your login ID or password.

In addition, do not share the answers to your security questions — even for what you think is a legitimate business need. Sharing login credentials opens the door to identity theft and unknowingly sharing confidential data.

6. Do Not…

Use the same password for every application.

Using one password for all of your applications is equivalent to having one key that unlocks every door in your life. If you use the same login information across all accounts, it won't take long for a hacker to identify numerous places they can apply your password and access your personal and company confidential information.

7. Do Not…

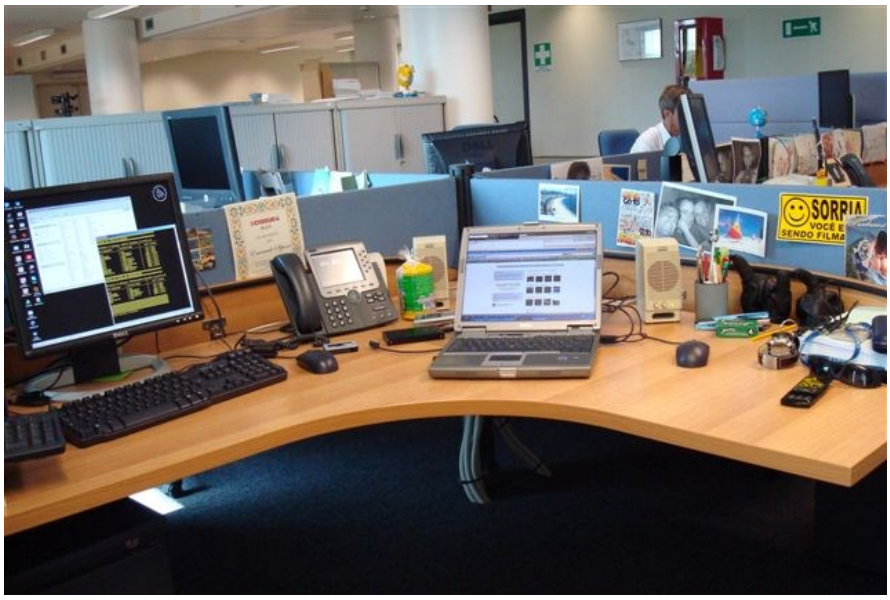
Store passwords on a piece of paper or other easily accessible document.

The issue with handwritten account details is that they're simply too easy to steal. Furthermore, these days most people are logging in at numerous locations, whether they be remote, traveling, in the office, etc. It isn't practical to leave this note locked away somewhere. Moreover, it isn't safe to carry a loose leaf piece of paper containing sensitive information with us wherever we go.

8. Do Not…

Leave your laptop or mobile device unattended while in a public place. Lost or stolen equipment, including mobile devices connected to corporate networks, should be reported immediately.

Leaving your device in plain view increases the risk of your property being stolen. If your device is stolen or lost, reporting this immediately can help protect sensitive and confidential information.



9. Do Not…

Keep open files containing personal or confidential information on your desk or in an unlocked file cabinet when away from your office/desk.

We recommend keeping confidential information locked away in a filing cabinet to prevent unauthorized users from gaining access. Be aware of how open your working environment is, and whether your files are visible to visitors, for example.

ABOUT EZE CASTLE INTEGRATION

Eze Castle Integration is the leading provider of IT solutions and private cloud services to more than 650 alternative investment firms worldwide, including more than 175 firms with $1 billion or more in assets under management.

When it comes to cybersecurity, we help clients:

- Develop Written Information Security Plans and Policies
- Move their IT to our highly secure Eze Private Cloud environment
- Fortify their existing IT environment.

The company's products and services include Private Cloud Services, Cybersecurity & Technology Consulting, Outsourced IT Support, Project & Technology Management, Professional Services, Telecommunications, Voice over IP, Business Continuity Planning and Disaster Recovery, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

To learn more about Eze Castle Integration, contact us at **800-752-1382** or visit **www.eci.com**.