

## IT Security DOs & DON'Ts Be Cyber Aware





#### **TABLE OF CONTENTS**

Security DOs3
---------------

Security	DON'	Тѕ		 	.14
occarrey			 •••••	 • • • • • • • • • • • • • • •	• • •



#### 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.

<b>F</b> -aCastla	Please log on
EzeCastle	User name:
INTEGRATION	Password:
	Log On

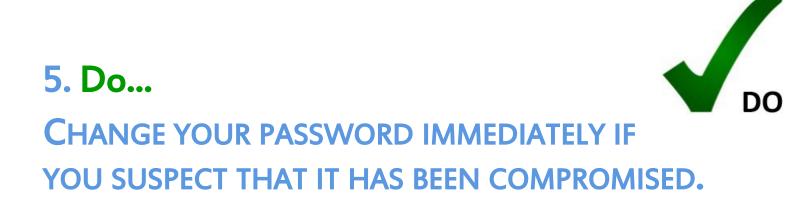
#### 4. Do...



#### 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).

Choose a password:	•••••••• 123456789 Minimum of 8 characters in length.	Password strength:	Weak
Re-enter password:			
Choose a password:	••••••• 98765432 Minimum of 8 characters in length.	Password strength:	Fair
	immuni or o characters in length.		
Choose a password:	•••••••• 987654321 Minimum of 8 characters in length.	Password strength:	Weak
Choose a password:	•••••••• 98765432A Minimum of 8 characters in length.	Password strength:	Strong



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.

Username	
email address	
Cancel	Reset 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.

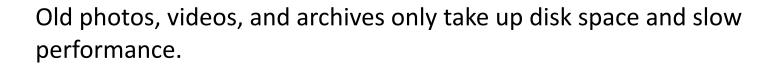




Waiting to report suspicious activity heightens threats and increases your chances of becoming the victim of hacking, system failure or data loss/destruction. Contact your IT team or Computer Security Incident Response Team (CSIRT) immediately to minimize risks.



### 8. Do... GET RID OF "JUNK"





DO

#### 9. Do... CHECK UP ON UNUSED SOFTWARE



See what your programs are actually doing. If nothing, uninstall. This will reduce potential malware 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.





# **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.





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.

5 X
Date: Mon, 02 Jul 2012 07:27:01 -0400           From: "A         " <a< td="">         @com&gt;           To: N/A         Subject: FW: FW: Carried Interest fees        </a<>
Charset utf-8*
Hello, I apologize for the late reply. Please find attached the doc. requested (regarding the NYSE crrie interest fees).
Regards, Alice Rogers
Capital Investors (not really) 212-555-5555
Quarter2012_8k_fees_NYSE.exe (352KB) Trojan.Win32.Agent



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.

524.2134	30215021569	01444587901	886524.2134	30215021569	01444587901	886524.2134	30215021569	01444587
54240404	87459823654	89564875564	54654240404	87459823654	89564875564	54654240404	87459823654	89564875
21404359	85123030213	02654895465	23421404359	85123030213	02654895465	23421404359	85123030213	02654895
53402213	13311123150	13025165465	78553402213	13311000011	13025165465	78553402213	13311125644	13025165
58672464	25468952654	76540215497	49758672464	25468952654	76540215497	49758672464	25468952654	76540215
68652031	78021328503	87654860216	97968652031	78021328503	87654860216	97968652031	78021328503	87654860
79561203	57920045685	54897564202	25679561203	57920045685	54897564202	25679561203	57920045685	54897564
56530979	48314904153	15465465460	26456530979	48314904153	15465465460	26456530979	48314904153	15465465
32031246	18946516746	21654 21000	610 0 2 0 3 1 2 2 0	100000000000000000000		1246	18946516746	21654621
56452123	51561687515	40216	7 C m DI	MSSIT	TT TTT	2123	51561687515	40216548
45754545	23162685421	56102		1626 4	لداسه الطوطور	4545	23162685421	56102165
91675425	62964975421	62165 54052	20503025495	62064025422	60165054050	265026 5425	62964975421	62165054
59782135	35656497652	13245450154	34659782135	35656497652	13245450154	34659782135	35656497652	13245450
23100002	31200124556	84987984301	64023100002	31200124556	84987984301	64023100002	31200124556	84987984
56462857	87976423120	24568765435	13656462857	87976423120	24568765435	13656462857	87976423120	24568765
45622256	31655976421	01235435435	55645622256	31655976421	01235435435	55645622256	31655976421	01235435
66566433	05234605242	43021648576	79866566433	05234605242	43021648576	79866566433	05234605242	43021648
23101346	59257561221	53441100000	59823101346	59257561221	53441100000	59823101346	59257561221	53441100
57242104	56024565237	00000001243	56457242104	56024565237	0000001243	56457242104	56024565237	00000001
68976543	85421245454	53727672034	23168976543	85421245454	53727672034	23168976543	85421245454	53727672
12124567	45456402124	25375763520	24212124567	45456402124	25375763520	24212124567	45456402124	25375763
12054976	24575454012	43597572672	54212054976	24575454012	43597572672	54212054976	24575454012	43597572
23051564	42245454440	40133727967	85323051564	42245454440	40133727967	85323051564	42245454440	40133727
46791630	55546520303	97801322479	65246791630	55546520303	97801322479	65246791630	55546520303	97801322
52675642	40555120245	69675014372	21352675642	40555120245	69675014372	21352675642	40555120245	69675014
21000231	21205512563	97846520434	13421000231	21205512563	97846520434	13421000231	21205512563	97846520
00000005	23564012452	52768975403	24000000005	23564012452	52768975403	24000000005	23564012452	52768975
24242412	54545450215	24214672732	42424242412	54545450215	24214672732	42424242412	54545450215	24214672
52424524	88879564501	03427679854	75452424524	88879564501	03427679854	75452424524	88879564501	03427679
01243424	55556523154	64031254596	97501243424	55556523154	64031254596	97501243424	55556523154	64031254



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.



DON'T



#### 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.





STORE PASSWORDS ON A PIECE OF PAPER OR OTHER EASILY ACCESSIBLE DOCUMENT.

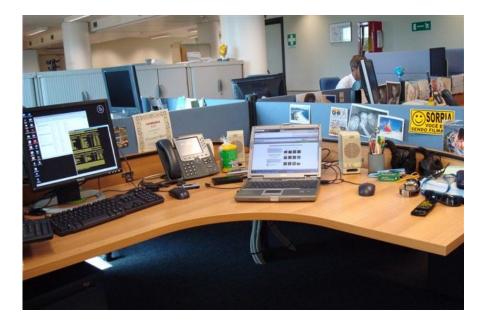
The issue with handwritten account details is that they're simply too easy to steal. Furthermore, these days most people are logging in at numerous locations, whether they be remote, traveling, in the office, etc. It isn't practical to leave this note locked away somewhere. Moreover, it isn't safe to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





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.





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.

#### Best Cyber Security Provider Waters Ranking 2016

EzeCastle

Active Threat Protection Cyber Consulting Phishing & Training Risk Assessments Written Security Plans & MORE

LEARN MORE >