YOUR PASSWORDS ARE JUST LIKE YOUR UNDERPANTS

CHANGE THEM OFTEN!

KEEP THEM PRIVATE!

NEVER SHARE THEM WITH ANYONE!
SEE SOMETHING STRANGE OR UNUSUAL?
REPORT IT IMMEDIATELY!

If you are worried about reporting a non-event, don’t be! Reporting anomalies does not mean you are reporting a non-event, it just means you are reporting something unusual.
In the case of incident reporting, it is always better to be safe than sorry!
KEEP A CLEAN DESK!

DON'T LEAVE PASSWORDS OUT IN THE OPEN.
LOCK YOUR SCREEN BEFORE LEAVING YOUR DESK.
PUT AWAY CONFIDENTIAL DOCUMENTS.
MESSY DESKS ARE SECURITY RISKS.

© THE SECURITY AWARENESS COMPANY
Don’t be phish bait.

- Use common sense.
- Stay focused.
- Slow down.
- Think before you click.
- If you suspect a phishing attack, report it immediately.
DON’T LET THESE COMMON PHISHING PHRASES CATCH YOU HOOK, LINE, AND SINKER!

NEW MESSAGE FROM: YOUR BANK
“FRAUD ALERT.”

NEW MESSAGE FROM: facebook
“YOUR ACCOUNT WILL BE DISABLED!”

NEW MESSAGE FROM: NETFLIX
“PLEASE UPDATE YOUR PAYMENT DETAILS”
SUBJECT LINE
RED FLAGS

Dropbox validate DocuSign
confirm (de)activate
urgent P.O. DHL account update
payment password FedEx quote
invoice document UPS purchase
verify file
important RFQ
verify
purchase
important

KnowBe4
Human error. Conquered.
Think
Before
You
Click

Human error. Conquered.

KnowBe4.com
To click without thinking is like driving blindfolded.

Always hover the mouse over the link to find out where it will take you.

www.maliciouswebsite.com/malware/122930182928192891
Can you spot a social engineer?

It’s not always easy.

Trust but **verify** the identity of whom you are speaking to.
Social engineers manipulate people into breaking normal security procedures.

Don't be a puppet!
Do you know what social engineering is?

They are the practices used to gain access to important or sensitive information in organizations by deceiving or exploiting people’s trust.

The attacker may assume another identity by pretending to be a professional from a certain area to deceive people - who, if untrained, can be easily manipulated.
Preserve your privacy.

Social networks are the primary sources of data collection for phishing attacks.

If your personal information is on the Internet, you may be a victim of criminals.

Review your security and privacy settings. Make as little as possible available to those who are not on your network.
Social media is full of half truths and quite a few flat out untruths. That person posting pictures of their perfect life probably doesn’t post about the messy parts of their life. That clothing ad with unbelievable prices that pops up in your newsfeed, you really should not believe. That cool person you met online might not really be who they say they are. Social media is a great way to connect but you must always remember that not everything is as it seems to be.
LIKE PINEAPPLE ON PIZZA,
BE WARY OF UNEXPECTED ATTACHMENTS.
DO YOU RECOGNIZE THE SIGNS OF A SPEAR PHISHING EMAIL?

To: undisclosed-recipients;

From: Susan Molar <susanmolar@gmail.com>
Subject: UNITED NATIONS ORGANIZATION
Date: June 18, 2013 6:22:40 PM CDT
To: undisclosed-recipients;
Reply-To: hansbruce@london.com

Dear EMAIL OWNER/Fund Beneficiary,

We have been authorized by United Nation secretary general, and governing body of the UNITED NATIONS Monetary Unit, to investigate the unnecessary delay on your payment, recommended and approved by your favor during the course of our investigation, we discovered that your payment has been delayed by corrupt officials of the Bank who are trying to divert your funds into their private accounts.

If you did receive your funds thru this means you advised contact with following information:

1. Your Full Name:
2. Address Where You Want the Courier to Send ATM Card
3. AGE
4. Occupation:
5. Telephone Numbers:
6. COUNTRY:

NOTE: You are advised to furnish Mr. Hans Bruce with your correct and valid details. Also be informed that the amount to be paid to you is £1,000,000.00GBP. We expect your urgent response to this email to enable us monitor this payment effectively thereby making contact with MR. HANS BRUCE as directed to avoid further delay.

Congratulations,

MR. KASSYM-JOMART TOKAYEV
DIRECTOR-GENERAL
UNITED NATIONS ORGANIZATION

Requests for personal or sensitive information are usually scams.

Promises of money, threats or alarming messages, deals too good to be true are common phishing email tactics.

Random capitalization, odd punctuation, misspellings and improper grammar are usually good indications that the email is a fake and should be deleted ASAP.

DON'T BE PHISHING BAIT.

© The Security Awareness Company