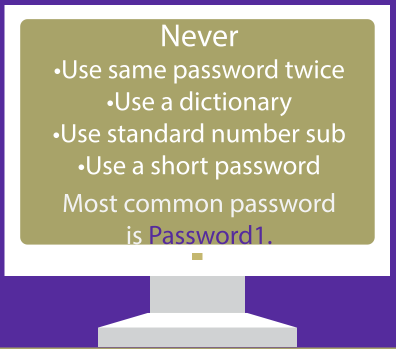
## Poor Passwords



Never
- Use same password twice
- Use a dictionary
- Use standard number sub
- Use a short password

Most common password is Password1.

## 15%

of physical security tests performed at client sites reported written passwords were found on and around user workstations.

## Peeping "Rom"

One in three workers leave their computers logged on to the network resources and unlocked when away from their desks.

## ALWAYS

- Enable two factor authentication when offered
- Give bogus answers to security questions
- Always report loss or theft to IT
- Keep your devices up to date
- Scrub your online presence

## A Little Too Social

70%

of young workers ignore corporate social media policies.

## USB Stick Up

60%

of users who find a random usb stick in a parking lot will plug it into their computer.

Add the company logo and that number increases to 90%

## 69%

of IT security pros say they come across phishing messages that get past spam filters

## ALWAYS

Scope links to see it's actual destination.

OR

Check the from email address & domain.

## "Phish" Biting

Users trained in avoiding phishing & scam emails fell for these malicious attacks

42% LESS

than those without training.

# *Security Info-graphic*

Common Phishing Scams:

- Bank notifications
- Online purchases
- Shipping notices
- Online dating
- PayPal account
- Facebook account

The Computer Man, Inc.

TCMI

EARTHBEND
YOUR EDGE IN TECHNOLOGY

## Hooking Up With Another Man's WIFI

Malware is often passed off as software updates on hotel internet connections.

## Reckless Abandon

70%

of users do not password protect their smart phones.

## 71%

of workers surveyed say they have been able to view a coworker or strangers work station in the workplace or a public place

## 89%

of people who find lost cell phones look at sensitive information

The average data breach costs

$12.7M

## 33%

of all security incidents can be attributed to employee carelessness

Never Give Personal Or Financial Data To People Overseas!

When In Doubt Contact Your Information Technology Department.

The average company requires 45 days of recovery after a security breach.

## 26.4%

of malware is key logger or application specific; which often requires detailed knowledge of or physical access to a targeted system

Sources: Linkedin SlideShare Blog, Sophos Labs

# IT Security
# DOs and DON'Ts

what to do | what not to do | what to look out for
what to report | how to stay secure

Security is the responsibility of us all. Follow the tips in this handbook and you’ll be helping to keep yourself, your colleagues and our business safe.

Security sets us free to do what we do best. It’s simple and mostly common sense.

Make sure you let your family and friends know what to do too, so they’re safe online.

# 1

# Don’t be tricked into giving away confidential information

Don’t respond to emails or phone calls requesting confidential company information—including employee information, financial results or company secrets.

It’s easy for an unauthorized person to call us and pretend to be an employee or one of our business partners.

Stay on guard to avoid falling for this scam, and report any suspicious activity to IT.

And protect your personal information just as closely.

2

# Don’t use an unprotected computer

When you access sensitive information from a non-secure computer, like one in an Internet café or a shared machine at home, you put the information you’re viewing at risk.

Make sure your computer is running the latest approved security patches, antivirus and firewall. And you should work in user mode, not administrator mode, whenever possible.

# 3

## Don’t leave sensitive info lying around the office

Don’t leave printouts containing private information on your desk. Lock them in a drawer or shred them. It’s very easy for a visitor to glance down at your desk and see sensitive documents.

Keep your desk tidy and documents locked away. It makes the office look more organized, and reduces the risk of information leaks.

# 4

## Lock your computer and mobile phone when not in use

Always lock your computer and mobile phone when you’re not using them. You work on important things, and we want to make sure they stay safe and secure.

Locking your phone and computer keeps your data and contacts safe from prying eyes.

5

# Stay alert and report suspicious activity

Always report any suspicious activity to the IT team. Part of our job is to stop cyber attacks and to make sure our data isn’t lost or stolen.

All of our jobs depend on keeping our information safe. In case something goes wrong, the faster we know about it, the faster we can deal with it.

# 6

# Password-protect sensitive files and devices

Always password-protect sensitive files on your computer, USB, smartphone, etc.

Losing items like phones, USB flash drives and laptops can happen to anyone. Protecting your devices with strong passwords means you make it incredibly difficult for someone to break in and steal data.

# 7

## Always use hard-to-guess passwords

Don’t use obvious passwords, like “password,” “cat,” or obvious character sequences on the qwerty keyboard, like “asdfg” and “12345.” It’s better to use complex passwords.* Include different letter cases, numbers, and even punctuation.

Try to use different passwords for different websites and computers. So if one gets hacked, your other accounts aren’t compromised.

*$e7enal1ig@t0r5inmyb^th
(seven alligators in my bath)

# 8

## Be cautious of suspicious emails and links

Don’t let curiosity get the best of you.

Always delete suspicious emails and links. Even opening or viewing these emails and links can compromise your computer and create unwanted problems without your knowledge.

Remember, if something looks too good to be true, it probably is.

# 9

## Don’t plug in personal devices without the OK from IT

Don’t plug in personal devices like USB flash drives, MP3 players and smartphones without permission from IT.

These devices can be compromised with code waiting to launch as soon as you plug them into a computer.

Talk to IT about your devices and let us make the call.

# 10

## Don’t install unauthorized programs on your work computer

Malicious applications often pose as legitimate programs, like games, tools or even antivirus software.

They aim to fool you into infecting your computer or network.

If you like an application and think it will be useful, contact IT to look into it for you before installing.

# An ongoing effort

Computers are here to stay, and that means threats are here to stay too. So this top 10 list will change over time as we encounter and overcome new threats.

# Social Engineering Red Flags

KnowBe4
Human error. Conquered.

## FROM:

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address **from a suspicious domain**? (like micorsoft-support.com)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

## TO:

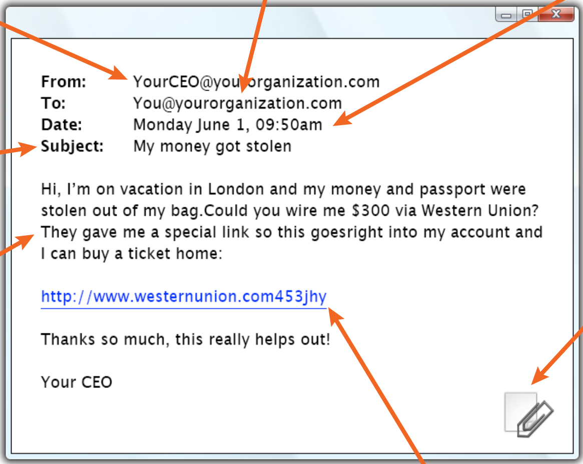
- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT:

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday June 1, 09:50am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

http://www.westernunion.com453jhy

Thanks so much, this really helps out!

Your CEO

## ATTACHMENTS:

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on is a .TXT** file.

## CONTENT:

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

## HYPERLINKS:

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r" & "n".