Security Awareness Training

The 2019 Essential Cyber Security Threat List

Simple & Effective
Security Awareness

Common Security Risks

This is a list of the most common security threats that your employees need to be aware of. There are of course more threats out there. This is just a starting point with the most common ones that should be the foundation of your training efforts. **Awareness training must be interesting** enough to get people‘s attention and short enough to be remembered.

Security awareness is a **compliance issue** and is needed to accommodate standards and regulations such as GDPR, ISO27001, PCI-DSS and many country or state laws. Security awareness is an **essential part of employee training** and is the most effective way to keep companies safe from intruders and hacks.

We hope this list helps to identify at least some of the threats that are around today.

The protection of confidential information is vital for every organization. The purpose of security awareness training is to develop competence and company culture that **saves money and creates a human firewall** guarding against an ever increasing threat of reputational and actual damage and data loss.

Essentials

A modern company needs informed employees who have a basic understanding of where security risks lie

Email

An understanding of phishing, malicious attachments and when it is proper to use email and when not

Internet

Safe browsing and understanding http or https, phishing sites, and common threats on the web

At the Office

How to safely handle confidential content, printed or digital, and the correct ways to store and dispose of it

Out of Office

Risk awareness when working from home using a laptop or a phone

Social Awareness

Understanding where the risks are and how social engineering works is essential to securing access to a workplace and data

Privacy

With increased regulations to guard personally identifiable information, mistakes can be very expensive

Mobile

Mobile phones today are mini computers that can hold valuable information

Data leaks

A data leak is the intentional or unintentional release of secure or private/ confidential information to an untrusted environment. Failure to report a leak can have severe consequences for the individual and lead to hefty fines for the company.

Essentials Privacy

Ransomware

Ransomware is malware or a virus that encrypts the data on your computer or in some cases your whole network. You cannot access your files or pictures until you pay the ransom, or sometimes not even then.

Essentials Internet

Phone Locking

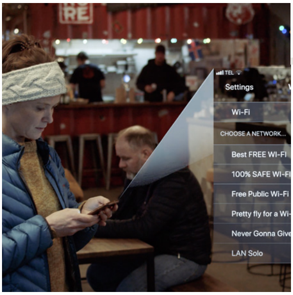
Documents, memos, email, and contacts can be stolen if you leave your phone unlocked. It is important to guard the information. Always keep your phone locked when you're not using it.

Essentials Mobile

Vishing

Vishing is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information thatwill be used for identity theft.

Mobile Social



Unknown network

It is very easy for a hacker to set up a Wi-Fi access point, but if you connect, much of your communication can be monitored or even manipulated.

Essentials Social

Mobile listening

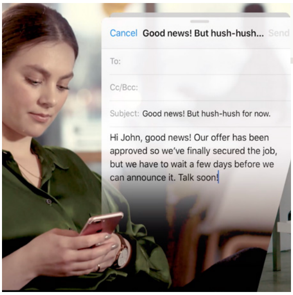
You should be aware that there might be a malware installed on your mobile where they can turn on your camera and microphone to listen in on your conversation.

Essentials Out of office

Doublecheck Before You Trust

There is always a possibility that someone has been “listening in” on your email conversations, jumping in when you least suspect it and fooling you into doing something you should not do.

Email Out of office Internet



Good news! But hush-hush...

To:

Cc/Bcc:

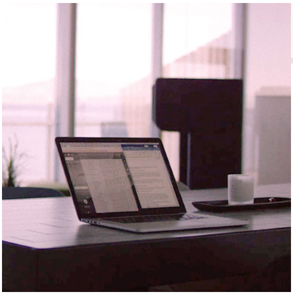
Subject: Good news! But hush-hush for now.

Hi John, good news! Our offer has been approved so we’ve finally secured the job, but we have to wait a few days before we can announce it. Talk soon!

Autofill

Often confidential information leaks out because email senders are in a hurry or distracted and select the wrong recipient.

At the office Email



Unattended Computer

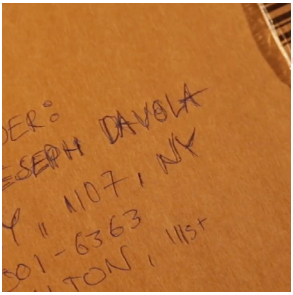
Leaving your computer unlocked and unattended can cause serious problems if someone else has access to it.

Essentials Privacy

Same Password

Managing multiple passwords can be hard, but it is essential to have different passwords for different sensitive accounts.

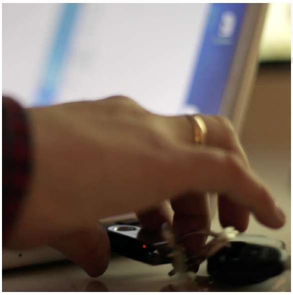
Essentials Mobile



Malicious Attachments

Email is still an important communication tool for business organizations. Attachments represent a potential security risk. They can contain malicious content, open other dangerous files, or launch applications, etc.

Essentials Email



Removable Media

Removable media is a common way to move larger amounts of data. The risks are numerous, including data loss, malware threats and mis-placement resulting in reputational damage.

Privacy Out of office

USB Key Drop

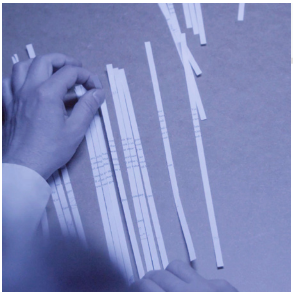
A USB key drop is when a hacker leaves a USB stick on the ground or in an open space, hoping that someone will plug it into their computer, giving access to their computer and all files they have access to on the network.

Out of office · Social

Social Engineering

Social engineering is the use of a deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes often tricking people into breaking normal security procedures.

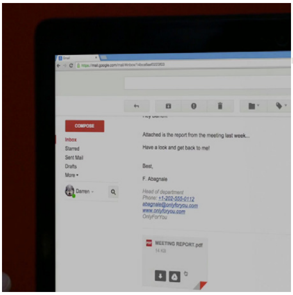
Essentials · Out of office · Social



Dumpster Diving

Dumpster diving is a technique to retrieve sensitive information that could be used to access a computer network. It isn't limited to searching through the trash for documents.

At the office · Social



Attached is the report from the meeting last week...

Have a look and get back to me!

Best,

F. Abagnale

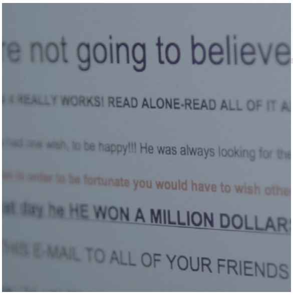
Head of department
Phone: +1-202-555-0112
abagnale@onlyforyou.com
www.onlyforyou.com
OnlyForYou

MEETING REPORT.pdf
14 KB

Spyware

Spyware and malware are types of software that enable a hacker to obtain covert information about another's computer activities by transmitting data from the computer or gaining direct access to it.

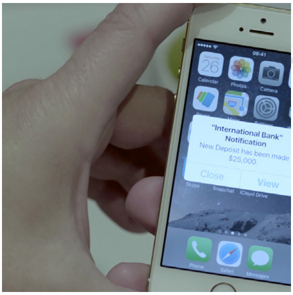
Essentials · Internet · Email


e not going to believe
REALLY WORKS! READ ALONE-READ ALL OF IT A
to be happy!!! He was always looking for th
be fortunate you would have to wish othe
day he HE WON A MILLION DOLLAR
IS E-MAIL TO ALL OF YOUR FRIENDS

Chain Letter

A chain letter attempts to convince the recipient to pass it on to others. The risk is that email addresses will be distributed to a malicious person, and the email can include links to malware.

✉ Email   At the office


"International Bank" Notification
New Deposit has been made $25,000
Close
View

CEO Scam

The CEO scam is when a hacker impersonates executives and tricks employees into sending sensitive information. This includes using social engineering to manipulate people and their actions.

Internet   Social

Clean Desk

Maintaining a clean desk includes not leaving sensitive documents on the desk, not writing passwords on sticky notes, cleaning sensitive information off a white board, and not leaving an access card where it might be stolen.

Social   At the office

Computer Installs

Keep software up to date to defend against serious issues. Viruses, spyware, and other malware rely on unpatched and outdated software.

Internet   At the office

Password

Choosing a good password is necessary. Choose one that has at least 8-10 characters and at least one number, one uppercase letter, one lowercase letter, and one special symbol. Do not use any words that are in the dictionary.

Essentials Internet

Password Handling

Choosing a good password is just a start. Use different passwords for different accounts and don’t leave the password where it can be found. Don’t send credentials by email or store them in an unsecure location.

Essentials Internet

Printouts

Printing documents and leaving them in the printer can give unauthorized persons access to confidential data.

Essentials At the office

Confidential Material

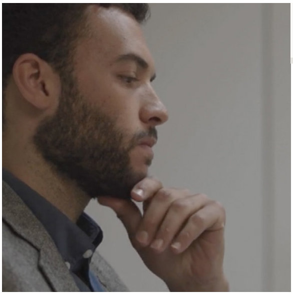
Private media is often not regulated and sometimes unsecure. Understanding the ways a hacker might gain access to unauthorized data is important.

Out of office At the office

Tailgating

Tailgating, sometimes called piggybacking, is a physical security breach where an unauthorized person follows an authorized one into a secure location.

Essentials At the office Social



Phishing

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Essentials Email Social

HTTPS

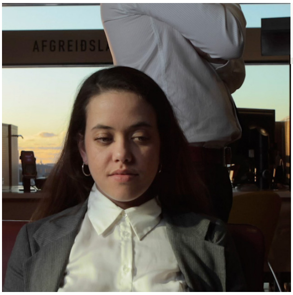
Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security to the data in transit.

Essentials Email Social

Spear Phising

Spear Phishing is the practice of studying individuals and their habits, and then using that information to send specific emails from a known or trusted sender's address in order to obtain confidential information.

Essentials Email Social



Shoulder Surfing

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder.

Essentials Social

Free WiFi

People usually use free WiFi without thinking. One of the most common open WiFi attacks is called a Man-in-the-Middle (MitM) attack, where a hacker can monitor all traffic and get sensitive information.

Out of office Internet

Home WiFi

Home networks are often set up in a rush to get connectivity ready as soon as possible. Most people do not take any steps to secure their home network, making them vulnerable to hackers.

Internet Out of office

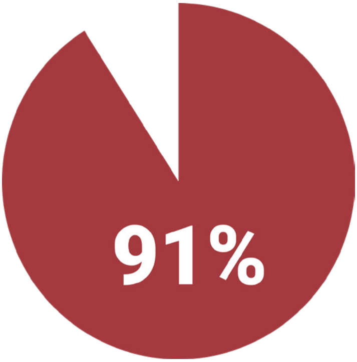
Keylogger

A keylogger is a piece of malicious software or hardware (a small device connected to the computer keyboard) that records every keystroke you make on a keyboard.

At the office

How to make your employees aware of the risks?

When defending your systems and software against cyber threats, technological solutions alone are not enough to mitigate the risks. Studies show that **91 per cent of successful breaches rely on human errors.**



Cybersecurity is now first and foremost about people. This means companies need to create and nurture a security culture with regular training and awareness reminders to all employees. No matter how up-to-date your systems and firewalls are (and they should be), you and your staff might be the weakest link when it comes to your company's cybersecurity. **It only takes one unaware employee to breach a company** resulting in an attack that could end up costing millions.

BE AWARE

If you are looking for a way to incorporate Cyber Security Awareness into your company's culture AwareGO has a simple and effective solution using short videos designed to keep up the cyber security awareness level. With no need for a complicated on-boarding procedure companies can **start awareness campaigns within minutes** with the simple and intuitive deployment *platform.*

About the List

This simple list is hopefully a helpful tool for security personnel or data protection officers when it comes to defending against cyber criminals and finding potential security risks.

We will try to update this list with new content as often as possible. If you feel that anything is missing, please let us know at awarego@awarego.com.

We think of security awareness as a marketing campaign instead of a training effort, it should be enjoyable.

Ragnar Sigurdsson

Founder & CEO, Ethical Hacker, CISSP

Ragnar has a first hand experience when it comes to the challenges organizations face when training employees on proper security measures. He saw people doze off and completely loose interest during security awareness training. This is why he started AwareGO in 2007: There had to be a better way to bring the security message to the masses and make workplaces safer.

AwareGO

Simple & Effective Security Awareness

At AwareGO we use marketing principles and humour to raise employee awareness and help companies be compliant with he latest updates and changes to cyber security standards and privacy laws. AwareGO follows what is happening in security today and provides organisations of all sizes with the tools they need to train their employees to keep sensitive data safe and secure.

Get In Touch

Phone

+354 899 4370

Email

awarego@awarego.com

Address

AwareGO, Borgartun 27,
105 Reykjavik Iceland

awareGO