security awareness news

the security awareness newsletter for security aware individuals

"BEST OF" Edition

Celebrating National Cyber Security Month

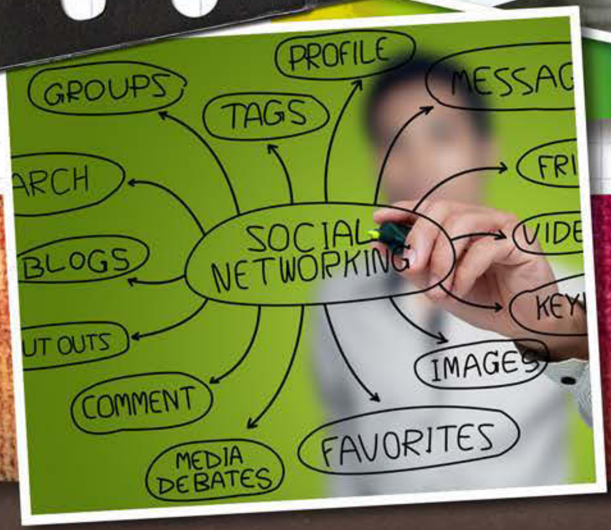
National Cybersecurity Awareness Month

A WORD FROM WINN SCHWARTAU

THE FOUNDER OF THE SECURITY AWARENESS COMPANY

The Security Awareness Company's Greatest Hits
A
Password - Losing Smartphones - ID Badges - VPNs
Pretexting - Home Networks - Social Networking
and more!

Security A to Z: A Dictionary



PRESENTED BY

THE SECURITY AWARENESS COMPANY

National Cyber Security Awareness Month is all about YOU.

Every October, we celebrate National Cyber Security Awareness Month, which was created by StaySafeOnline.org and is supported by organizations all over the world, including the Department of Homeland Security and Microsoft. Get your company, your family, and your friends involved this year to help spread security awareness to everyone everywhere and make this online world safer.

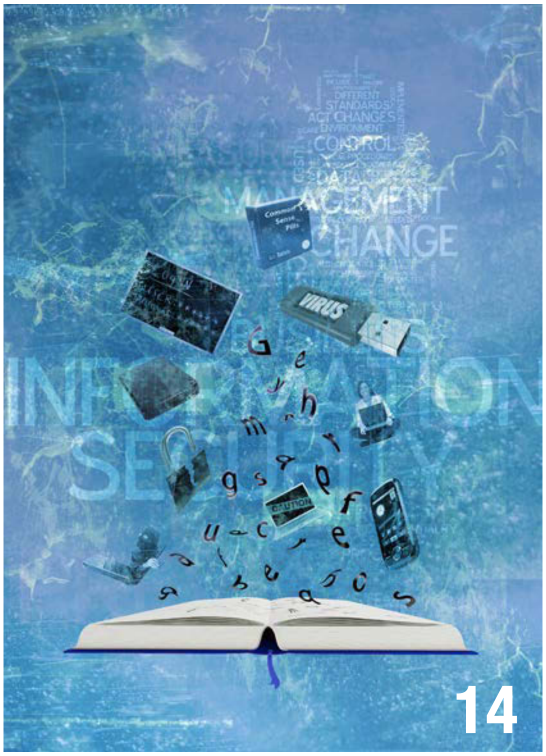
October

National Cyber Security
Awareness Month

staysafeonline.org

content

4


MANAGEMENT
CHANGE
CONTROL
VIRUS
INFORMATION
SECURITY
14

http://www.
scam!
User
Password
18

6

20

A Word from Winn

The Security Journey

You are a big part of any security effort and this Best Of Special Edition should help guide you on your journey. The best thing any of us can do to maintain a high level of security is to just be Security Aware. It isn't anything technical nor should it feel overwhelming. It is simply about becoming aware of your surroundings and reacting in a common sense way. A security aware person is alert and involved every day, with every step, every action, BECAUSE: **Security is the journey, not the final destination.**

After thirty years in the security industry, I am more challenged than at any time in my career. Why? Mobility and The Internet of Things. Today:

- We have 2+ billion fixed intelligent endpoints.
- We already have 2+ billion mobile intelligent endpoints.
- By the end of 2014 we will have 4+ billion mobile endpoints.
- By the end of the decade, that number will have increased to 20+ billion.

That's a lot of Internet "Things" to manage and use – securely. And what have I seen? The same three things that have plagued IT and the security industry since I first got involved almost 30 years ago:

- Apathy ("I don't care or need security…")
- Arrogance ("It'll never happen to me/us…")
- Ignorance ("I thought these devices were already secure…" & "I didn't know…")

So, after three decades, we are still trying to get the same messages to our user community, whether they are in the office, on the road or at home.

In most ways, nothing has changed. The basics are the basics even though the technology has changed. On the other hand, the very nature of how we protect networks should be changing more than it has – because things are changing so incredibly quickly.

Not so many years ago companies asked themselves, "Should we even connect to the Internet?" Today they ask themselves, "I wonder what devices are connected to our networks…?"

I have maintained for all of these years some simple mantras to make life more safe and secure.

- Trust But Verify.
- If it's too good to be true… you're being conned.
- Know all of your options.
- When in doubt, Ask! None of us know everything about everything.
- Use your gut about what is 'right' and 'wrong'.
- Pretend your Aunt Libby is looking over your shoulder as you make choices.

At The Security Awareness Company, we continue to be successful and our clients keep coming back because we have taken a unique view:

Security awareness must be personal, first and foremost. It must spawn a visceral response that challenges the user/student to get involved and care. We teach your staff how to protect their families and loved ones…and make those same issues relevant at the office. We rely on interactivity and entertainment to keep security interesting, not the typical eye-glazing, industrial, strict fact, non-imaginative content often chosen by the more technically based folks.. We are strong on real-world metaphor and examples to make your users care about security and privacy in ways that the most non-technical people can relate to.

We hope that this "best of" issue of our monthly newsletter, supporting National Cybersecurity Awareness Month 2012, will give you an idea of how we do things.

- Try our 'freebies'!
- See our NEW! Security Express Videos.
- Check out our art styles.
- Take our sample courses.

And then, give us a call.

I travel the world and my incredible staff has had the honor and opportunity to work on awareness issues in more than 20 countries, with every major branch of the U.S. government and countless other agencies across the globe. I am personally involved in or approve the content of all of our clients' products and projects,, especially for branding and customized programs – because I love it.

Winn Schwartau
Founder and CEO

Passwords

*If you listen to many security experts, they maintain that "Passwords are the worst form of authentication you can pick… yet we are stuck with them." What's **wrong** with passwords?*

1 Fundamentally, strong passwords are hard for bad guys to guess, which is excellent. However, this means they are probably difficult or impossible for us to remember.

2 With hundreds of credentials needed and the simple fact that you should NOT use the same password on multiple applications and websites, password management can be a nightmare. Somewhere, someplace, you need to keep a 'secure' record of them.

3 You have to enter passwords into a keyboard or other device, which means that they can be stolen with malware that records keystrokes.

4 Passwords travel down wires, often unencrypted, making them subject to interception.

5 Entering passwords over unencrypted WiFi hotspots can lead to a security and privacy nightmare.

6 Passwords are static, so attackers have a bigger window of opportunity than with other authentication techniques.

With so much working against them, it makes us wonder: what's ***right*** with passwords?

1. They are cheap to implement.
2. They require no special hardware.
3. Cut and Paste can be used.
4. They are easy to change.
5. They can be used on almost any platform.
6. There are no privacy worries about unique personal identifiers as with retinal scans and fingerprints.

So, since we're stuck with them for a while, what can we do to make passwords more effective and less risky, whether at home, at work or on the road?

Follow the Basics

You've heard this before and will no doubt hear it again. ***Do not share your User_ID or password with anyone, ever***. Not even with your boss or any administrator. There is never a need to share any password with anyone including your bank, eBay or any other online personal or professional associate.

If your password is compromised, you have essentially lost your online identity. Someone can do dastardly, nasty things in your name. At work, you could be suspected of doing something wrong or even illegal just by allowing someone else to use your password! They then become YOU and whatever they do reflects upon you.

Never respond to an email or phone call – EVER – asking you for your password(s).

Don't forget to change them on a regular basis. Do this at home with your online accounts. At work, ***ALWAYS follow corporate password management policy***.

Here's a Good Trick to Use

One of the best tricks for making a password easy to remember and hard to guess is to make up your own simple formula. For example, use the first letters from a familiar song or book and mix them with other familiar numbers. Use your imagination. It's quite simple, can even be fun and is very secure.

C1O2M3P4A5N6Y7
(COMPANY with numbers)

mmwbim1929
(My Mom was Born in Michigan, 1929)

s*o*t*r*##
(Somewhere Over the Rainbow)

ibahdn1964
(It's Been a Hard Day's Night, 1964)

Here you can see some great examples of the kinds of passwords NOT to use.

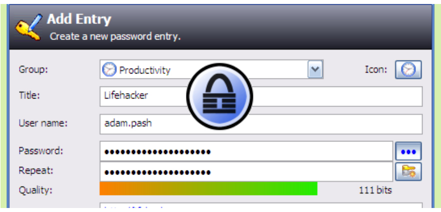
12345
AdminAdmin
Password1
Bob123
your birthday
license plate number

Use Some Type of Password Vault

With so many passwords, a simple way to protect *your* passwords is to create and hide a password protected Word or Excel file. It's not perfect, but is certainly much better than writing them down on a piece of paper.

Small software programs called *password vaults* are a popular way to securely store login information. They can greatly simplify the process of managing lots and lots of passwords.

At work, make sure you **know and follow corporate password management policy** and be sure to ask if you don't know *exactly* what is expected of you.



Add Entry
Create a new password entry.

Group: Productivity
Icon:
Title: Lifehacker
User name: adam.pash
Password: ••••••••••••••••••••
Repeat: ••••••••••••••••••••
Quality: 111 bits

9 Easy Ways to Protect Yourself Online

There is no perfect security. Never has been. Never will be. Some folks prefer not to get on social networking sites for many reasons, including: protecting their kids and family from online predators, wasting time and worries about identity theft. This is the choice we all have.

So, what should you do? The truth of the matter is – a lot. A lot of awareness and attention to details.

Limit the Info You Post

If you post your real name, birth date, address and phone number, you have essentially given away your identity. Your social security or identity number is a few clicks away.

Women hoping to connect with old friends often put their maiden name online. And we have multi-generation family members on many social networking sites. But, a mother's maiden name is often used as a security validation question! Avoid that one, request another option and pick another that is less public.

Don't talk about your specific schedule or routine. Don't use Facebook walls to set up small personal meetings like lunch with mom. Send a **private message** only. Remember the movie Home Alone? Bad guys know how to scout both physical and cyber neighborhoods.

Photos of friends and family are great, but they can also provide information to the bad guys. Make sure that **geo-tagging** on your mobile device is turned off; the bad guys know how to retrieve that information and figure out where you, your home or your loved ones are.

The internet is a public resource – not a private, quiet table for intimate conversation. Treat it as if everything you post will appear on CNN tomorrow. (It might and for some folks, it HAS!)

Do You Let Strangers Just Walk In?

Don't accept every invite to be a friend or contact. Invites should be from someone you actually know or should include a personal note. This obviously makes that friendship more personal – and real. (Whatever happened to the 'personal' part of friendship?) If you interact online with people you do not know in the physical world, be extra cautious about the amount of information you reveal.

First time physical meetings between online friends can go well, or not. It's a huge risk that must be well thought out, highly public in a controlled area, preferably after other types of contact like the phone or video chat. Still, be careful.

And most importantly, teach your kids and family about social networking security and privacy settings as well as the real risks of strangers on the internet. A little dose of paranoia is a good thing.

Be Skeptical

People lie. We all do. 5'9" tall and balding becomes 6'1" with rock star hair. Photos lie. Videos lie. Married? Single? You have to love

Treat the internet as if what you post will appear on CNN tomorrow. Skip detailing your life in a public forum (you're not Kim Kardashian!) to protect your online identity and reputation. Going out of town for two weeks? Don't say so online! Got a new email address? Don't post it on your wall! Feel like cursing your favorite football team? Probably best to refrain. You never know who can see what you put out there. And once you put it online, it is ALWAYS there.

the "It's Complicated" option on many sites.

Not that this is all malicious, either. It's human nature to put a best foot forward. Comments can be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and verify information before taking any action.

Do You Know Your Settings?

The better sites have tons of privacy settings options. Learn them. Apply the rules you want to use. Evaluate them every few months. If the site changes its rules, go in and see if your settings were affected.

The default settings for some sites may allow anyone at all to see your profile (Public) so you should customize your settings to restrict access to only certain people. There is still a risk posting sensitive information that only close friends can see: they, too, can cut and paste (innocently or otherwise) and suddenly it becomes public.

Be Wary of Third-Party Apps

Third-party applications (games, contests, surveys) may be fun, and they may waste time, but they may also be hostile. Use common sense. Research the application before downloading or engaging in the app. See what others say about it first, so you're not a victim or a guinea pig.

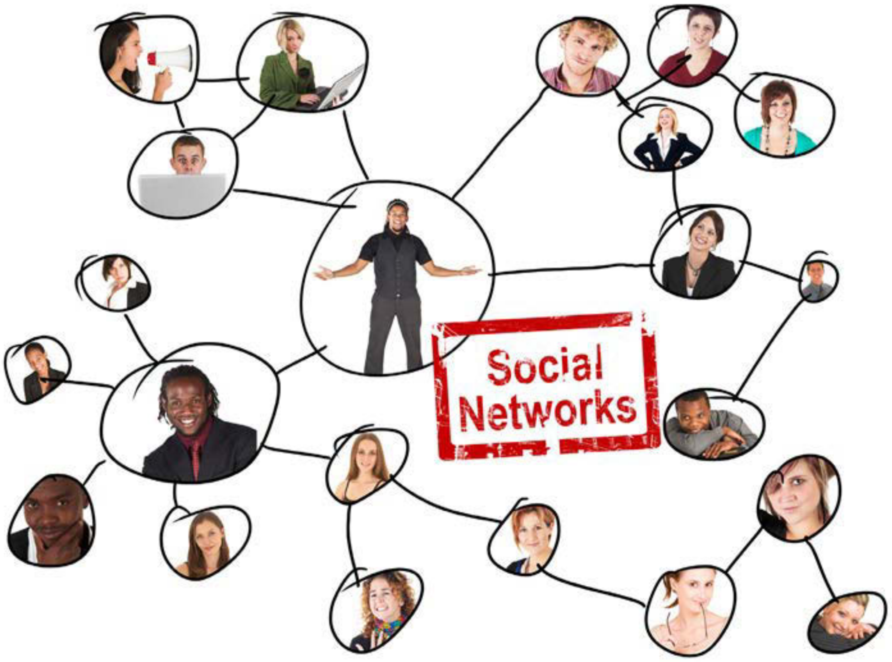
If is smells suspicious, don't use it. If it wants access to your personal data, modify your settings to limit it, or don't use it at all.

Use Strong Passwords

You've never heard this before! Right? We hope you have, but in case you haven't, here is the simplest password rule: Hard to Guess and Easy to Remember.

We know it's harder, but do NOT use the same passwords for all of your online accounts. Banking and sensitive sites, notably those also accessed from mobile devices, should have carefully crafted passwords, pass phrases or login credentials.

If your password is guessed, stolen, lost or otherwise compromised, someone else may be able to access your account and pretend to be you. Then everything they do is in your name.



A secure password vault is a simple and inexpensive way to manage lots of passwords. Initially setting it up can be time consuming for those of us with 100-1000 online accounts, but the security is worth it.

Data Use Policies

Do you own your name? Your identity? Can a social networking or other online presence claim to own your page and everything you post? You need to know what they say in their privacy area:

- Will they share information such as email addresses with other companies? (More spam!)
- Can they resell or share your posts, pictures and videos with other sites? (Identity theft concerns).
- Do they share your preferences and content with others to enhance targeted ads? (Spam, privacy concerns?)
- Does their referral policy automatically sign your friends up for spam? Some sites will continue to send email messages to anyone you refer until they join.

Your Computer

It's still the basics:

- Keep software, particularly your web browser, up to date. Browsers are the main, most vulnerable targets these days.
- Unless you need Java, turn it off.
- Many operating systems offer automatic updates. If this option is available, you should at least consider an update and see if it's worth it. Some updates and patches cause more problems than they solve.
- Use and maintain anti-virus software.
- Have separate user accounts at home. Only use the ADMIN account when making system changes.

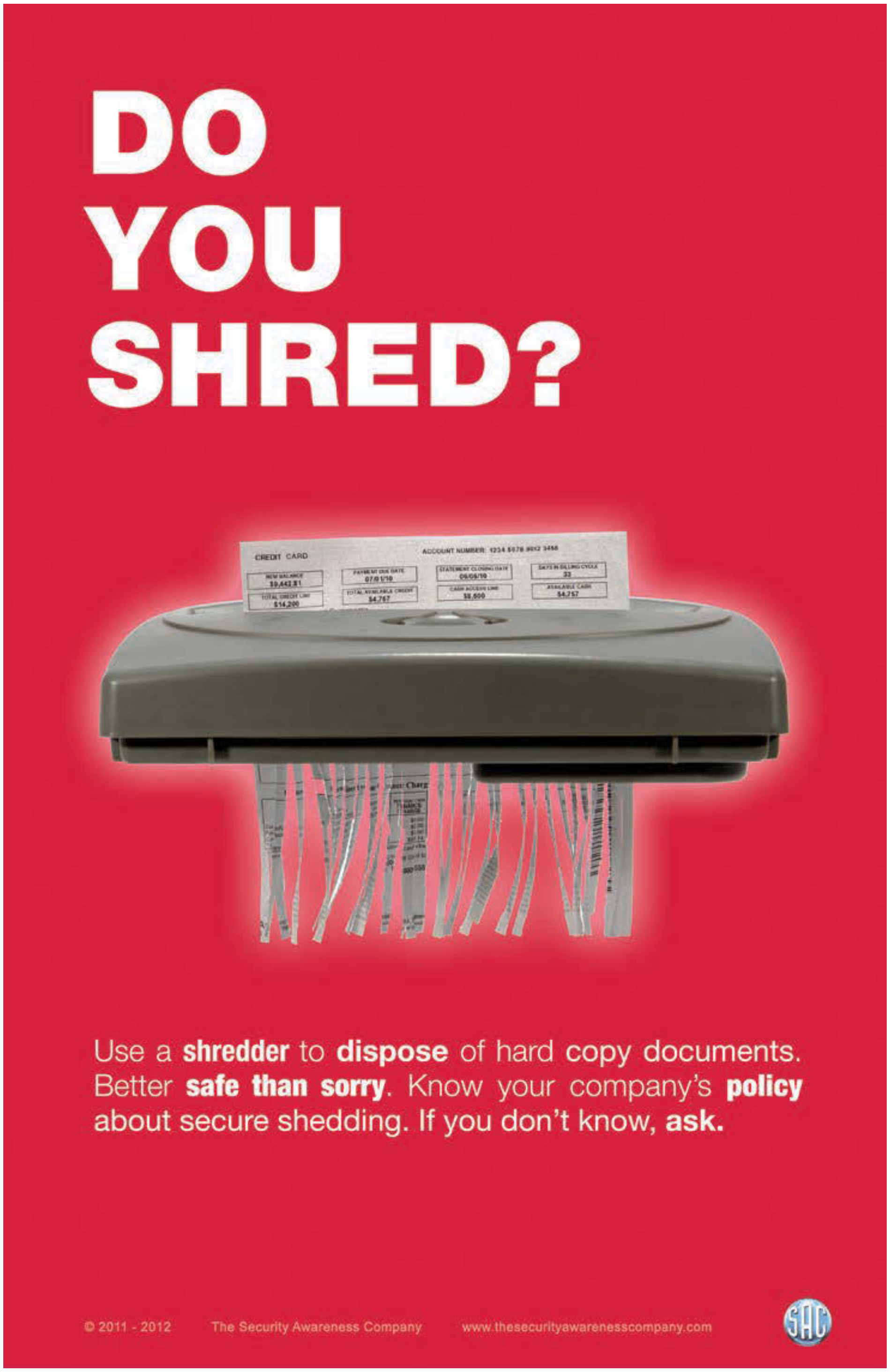
Are the Kids *Really* Alright?

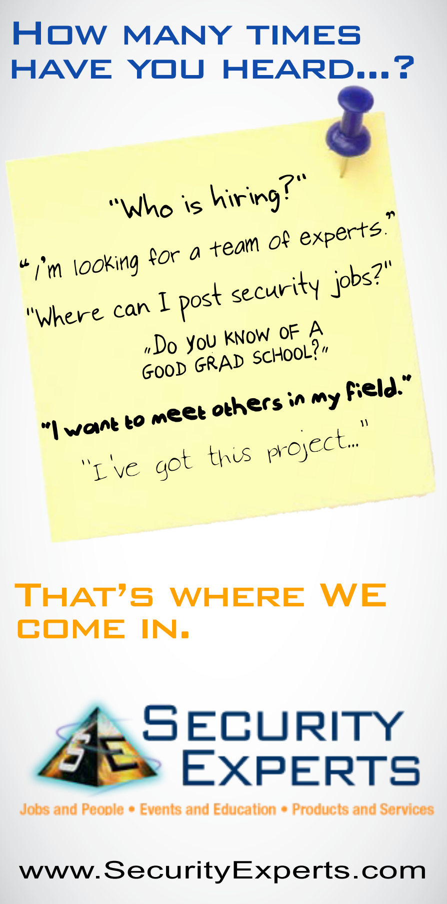
Children are especially susceptible to the threats that social networking sites present. Children are more trusting. They are more easily enticed. We teach them to respect adults and authority, but on the internet, no one knows who someone else really is.

Some sites have age restrictions, but children will often misrepresent their ages to join. All they have to do is enter or click on the appropriate age or birth date.

Teach your children about internet safety. Monitor, with respect and honesty, their online habits. Encourage and guide them to utilize appropriate sites.

It's up to parents – and only they can make sure that the children become safe and responsible users.


DO YOU SHRED?
CREDIT CARD
ACCOUNT NUMBER: 1234 5678 9012 3456
Use a shredder to dispose of hard copy documents. Better safe than sorry. Know your company's policy about secure shedding. If you don't know, ask.
© 2011 - 2012
The Security Awareness Company
www.thesecurityawarenesscompany.com
SAC



"Who is hiring?"
"I'm looking for a team of experts."
"Where can I post security jobs?"
"Do you know of a good grad school?"
"I want to meet others in my field."
"I've got this project..."

Awareness Artwork

SAC has a large inventory of entertaining and educational security awareness artwork that will keep your employees' minds focused on awareness issues. Take a look at our ever-growing collection online. There are many different styles to choose from. http://thesecurityawarenesscompany.com/artwork/artwork.html

Don't see what you need? Well, you're in luck: just contact us and we'll take care of it! We can create custom artwork for your needs!

Yes, We Do Need Badges

ID use is everywhere. Airports. Hotels. To buy beer. At school and of course, at work. It is part of physical security at work. Proper Photo ID credentials are given to trusted employees, providing them with tremendous access. Personnel who are issued a Photo ID badge are generally required to wear their photo identification at all times while on premises.

If you see someone on company premises without a visible badge, do you know what to do? Or if they are roaming around in a secure area with the wrong badge or unescorted? Make sure you know what to do!

Should you share your badge with another employee? Whatever s/he does is then in your name. The same goes for sharing computer, network and company resource passwords.

And So Do the Bad Guys

Are you allowed to wear your ID badge when not on the company premises? Should you? Do you know why or why not?

The bad guys are smart.

We know that none of you would alter your badge in any way, but others might! With only a zoom lens and a copy of Photoshop, badges can be photographed and then cloned. Pretty simple – and effective.

Therefore we strongly encourage you to know the rules about when to remove and stow your badge in a pocket or purse.

Lastly, if you lose your badge, **do you know what to do?**

Do you ever engage in **tailgating**? We all want to be polite, but we need to be exceedingly careful about allowing people to follow us into restricted areas or through **secure access points** – even if they have a badge. Most policies suggest that you politely explain that for security reasons, each person must enter on his or her own **credentials**.

National Cybersecurity Awareness Month

This October marks the 9th year of the National Cybersecurity Awareness Month, sponsored by the Department of Homeland Security. The purpose of this month is to spread awareness of an issue that applies to every single person who ever uses a computer or goes on the internet: Security Awareness.

Security Awareness does not imply anything technical. You don't have to know how computers work, or how to fix them when they break. You just need a healthy dose of common sense and to be aware of the many dangers both in the cyber and physical worlds that can inhibit your online security.

What do we mean by your online security? Your online identity, your passwords, your electronic data, your email and any form of activity you do that requires an internet connection.

We, at The Security Awareness Company, want to help promote Security Awareness to everyone - from the uber tech savvy to the grandparents who were forced to join Facebook. Enjoy this free issue of our monthly security awareness newsletter and use this month practice being a security aware individual.

Monthly Security Awareness Newsletters: From $595
The Security Awareness Company

Do your employees like THE OFFICE? Then they will love

MULBERRY.

Mulberry is a security awareness sitcom in the mockumentary style made popular by The Office and Parks & Recreation. Choose any or all of 12 episodes.

01. Intro (6:38)
02. Passwords, pt. 1 (5:26)
03. Passwords, pt. 2 (5:09)
04. Email, pt. 1 (6:51)
05. Email, pt. 2 (5:53)
06. Phishing (5:40)
07. Physical Security (6:32)
08. Policies (7:42)
09. Social Engineering, pt. 1 (6:44)
10. Social Engineering, pt. 2 (7:09)
11. Safer Browsing (6:01)
12. Conclusion (7:50)

Want to see a preview? Click here.

53% of malware is now delivered via internet download versus just 12% via email.

From a cybercriminal's perspective, tricking users into downloading and installing malware is a preferred means of attack since the weakness they are exploiting is the naiveté of their victim; this enables criminals to cast a wide net since there are no technology dependencies. In contrast, drive-by attacks require the user's computer to be vulnerable to the exploit being attempted.

Newsletters • Online Training • Custom

SAC

The Security Awareness Company
Entertaining. Educational. Effective.

Contact us today and learn about getting your own branded online security awareness school

Who Ya Gonna Call?

727.393.6600 • www.TheSecurityAwarenessCompany.com

Just for Losers

We love our mobile devices. We can stick them in our briefcases, purses, back packs, etc. and just keep on being productive, no matter where we are going. Many of us just don't feel 'complete' without a mobile device in tow.

But the smallest of these computing devices - our iPhones and other smartphones - are in some ways, like… well… socks! Maddeningly, they fall into cracks in couches, under pillows, under books and piles of stuff. All too often they simply disappear into that same black hole where so many socks have apparently gone.

As frustrating as it is to lose socks, losing a smartphone is certainly much more serious. Socks don't have personal data stored on them – except perhaps some remaining DNA from your last jog.

Smartphones store personal data. And they store company data. And, unfortunately, millions of users keep a list of their commonly used passwords in their device's 'Notes' app. This is just another reason you should have a separate, safe, secure place to keep all your passwords, passcodes and secure credentials.

Last month we discussed the disturbing findings by Symantec: More than 96% of 'lost' phones had their data accessed by the 'finders.'

So what do you do you to protect your mobile devices in these worst case scenarios?

Make sure you have a real-time backup of your data and contacts. Use the free service that usually comes with your phone contract and if you need, pay the few extra dollars for more storage capacity.

Don't use your smartphone as a storage device for your passwords and other security credentials.

Use a strong password on every mobile device you have. Yes, it's a pain. Yes, it slows you down by 1-2 seconds. But yes, it can save you from an incredible nightmare, if/when you become one of the below statistics.

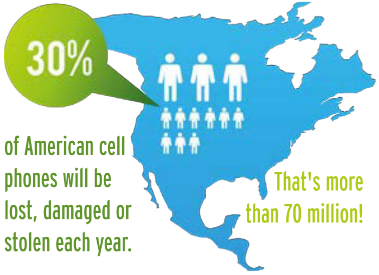
It's that important.

In the event you do lose your smartphone, you should contact your service provider quickly and have the device shut down. Also, if your device is equipped with a GPS tracker, your provider may be able to help you locate it.

NOTE: Make sure you know and follow company policy in the event that you lose any company issued or registered mobile device(s). And if you are permitted to BYOD, or Bring Your Own Device, make sure you adhere to company policy and procedure when using and transporting your device.

Did You Know..?

According to answerbag.com



of American cell phones will be lost, damaged or stolen each year.

That's more than 70 million!

120,000

smartphones are lost in Chicago taxis every year.

113 cell phones are lost or stolen every minute in the U.S. Multiply that by at least 10 to get global figures.

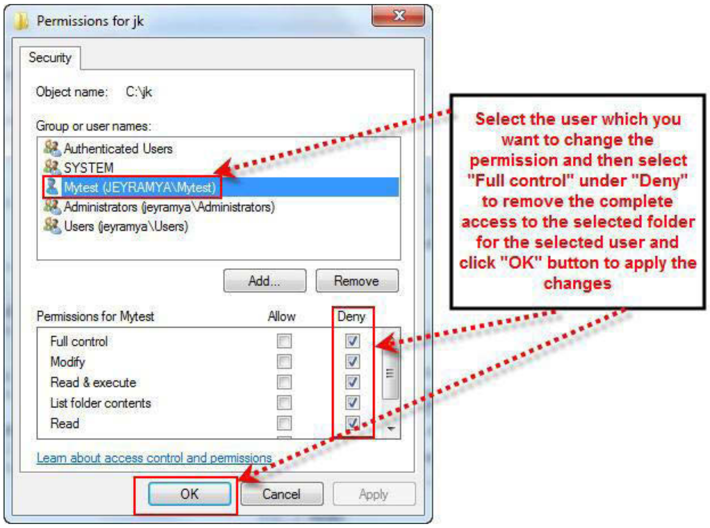
That's nearly 600 million lost phones around the world every single year.

Who's the Boss on Your Home Computers?

So, we have been talking about home networks, multiple computers, multiple users, etc. Many of us share computers at home and that's not a security problem. Unless, you aren't managing them correctly.

Here are a few tips to help you manage your multi-user computers.

- ☑ There should **only be 1 person** with administrator access, per computer. One big boss. That account should only be used when there are changes being made to the computer. A backup administrator is also a good idea.
- ☑ Each user should have his/her **own user account**, with individual login credentials. Set up as many as you want!
- ☑ **Sharing between accounts** and files should be set by the admin (Mom? Dad?) based upon your family's policies about who is allowed to do what.
- ☑ Learn how to set **parental controls** for each operating system.
- ☑ Configure browsers for each user to **filter content** as you deem appropriate.
- ☑ Consider adding additional **parental control software**, if you choose.
- ☑ Engage **the entire family**. These are security issues… not an invasion of privacy or lack of trust.



Permissions for jk

Security

Object name: C:\jk

Group or user names:

Authenticated Users
SYSTEM
Mytest (JEYRAMYA\Mytest)
Administrators (jeyramya\Administrators)
Users (jeyramya\Users)

Add... Remove

Permissions for Mytest	Allow	Deny
Full control	☐	☑
Modify	☐	☑
Read & execute	☐	☑
List folder contents	☐	☑
Read	☐	☑

Learn about access control and permissions

OK Cancel Apply

Select the user which you want to change the permission and then select "Full control" under "Deny" to remove the complete access to the selected folder for the selected user and click "OK" button to apply the changes

VPNs: Make Connections SECURELY at Home and Away

Virtual private networks, or VPNs, tend to get a bad rap as being difficult to set up, erratic in performance, and a questionable deterrent against possible security breaches.

Not true anymore.

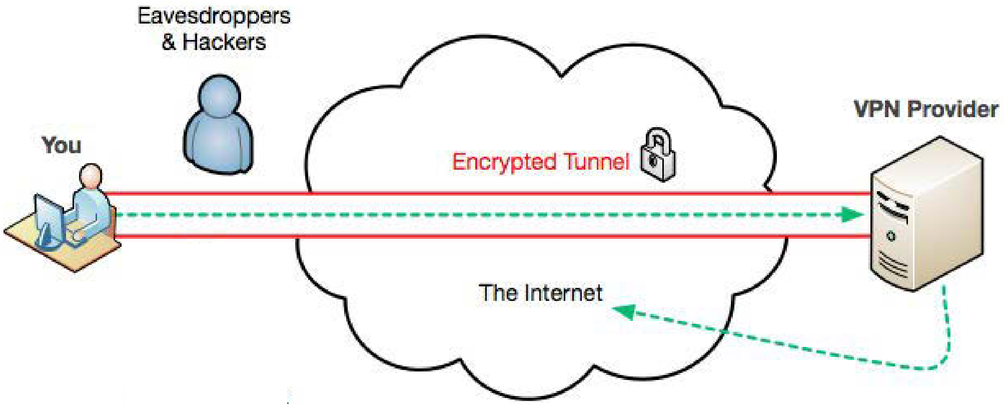
Products such as HMA achieve high levels of security and privacy, and are no more difficult to use than email. In fact, many experts argue that personal VPNs are no longer optional, but are absolutely necessary.

With endless travel, wireless hotspots, and other public internet access, the risk of bad guys grabbing your data and credentials must be dealt with by each user. Think of a VPN as an insurance policy; sure, most of time no one will be listening. Most of the time, you don't crash your car, either. It's just that one incident — that one car crash, that one electronic eavesdropper — when you desperately need the insurance afforded by a VPN to avoid a huge loss in confidential and valuable data.

A VPN encrypts all of the internet traffic in and out of a computer, and also hides the true location of the computer. Personal VPN services cost between $40-$100 per year and are worth every penny for the peace of mind.

You will be able to choose which VPN server you want to connect through. Some services offer hundreds of options, so your computer might appear to be in France or Japan or Australia while you are actually at an airport in Houston or London.

The Bad News: Some VPN services will slow down your internet experience. Read the reviews (http://myvpnreviews.com/), do some research, and if you don't like it within the first 30 days, most reputable companies will refund your money.

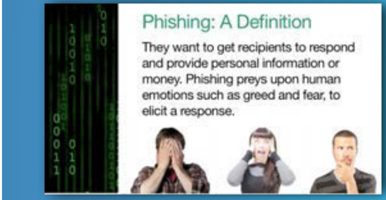


TWO GREAT NEW WAYS TO TRAIN YOUR EMPLOYEES

Two brand new, fun-to-watch short and affordable training options. Brand them with your company name for a small, additional fee. Mix and match or buy a package. Call us today to discuss your options. 727.393.6600

SECURITY EXPRESS

60 - 120 second security videos in byte-sized snippets!


Phishing: A Definition

They want to get recipients to respond and provide personal information or money. Phishing preys upon human emotions such as greed and fear, to elicit a response.

THREE-QUARTERS OF INCIDENTS INVOLVING LOSS OF SENSITIVE DATA ARE CAUSED BY FAILURE & HUMAN ERROR.

- ☑ Phishing Examples
- ☑ The ATM Attacks
- ☑ Keeping Sensitive Information
- ☑ Social Engineering Definition
- ☑ Data Loss: The Insider
- ☑ TMI Voicemail
- ☑ What is a Firewall?

These byte-sized snippets can be delivered in a number of formats (.mov, .mp4, .avi, .wmv, etc.) so you can use them in whatever way is best for you. Keep your employees entertained and engaged with a variety of video styles. Choose from our ever-growing catalog.

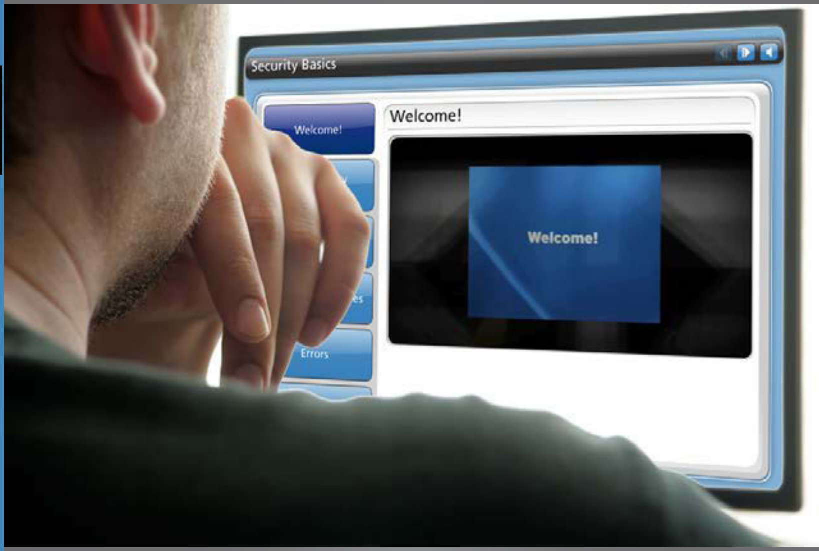
Buy them in groups of 3, 6 or 12 to build the perfect security awareness video playlist!

Call us today for more information!

MINI-COURSES

NEW!

5 - 8 minute interactive security awareness courses that use the same format as our full-length courses. They're designed to keep users engaged and to fulfill your training requirements!



- Passwords
- Backup
- Secure Internet Behavior
- Phishing
- The CIA Triads
- Company Policy
- Identity Theft
- Privacy
- Social Media
- Data Loss
- Authentication Basics
- Data Classification

More coming soon! We're constantly adding to our inventory.

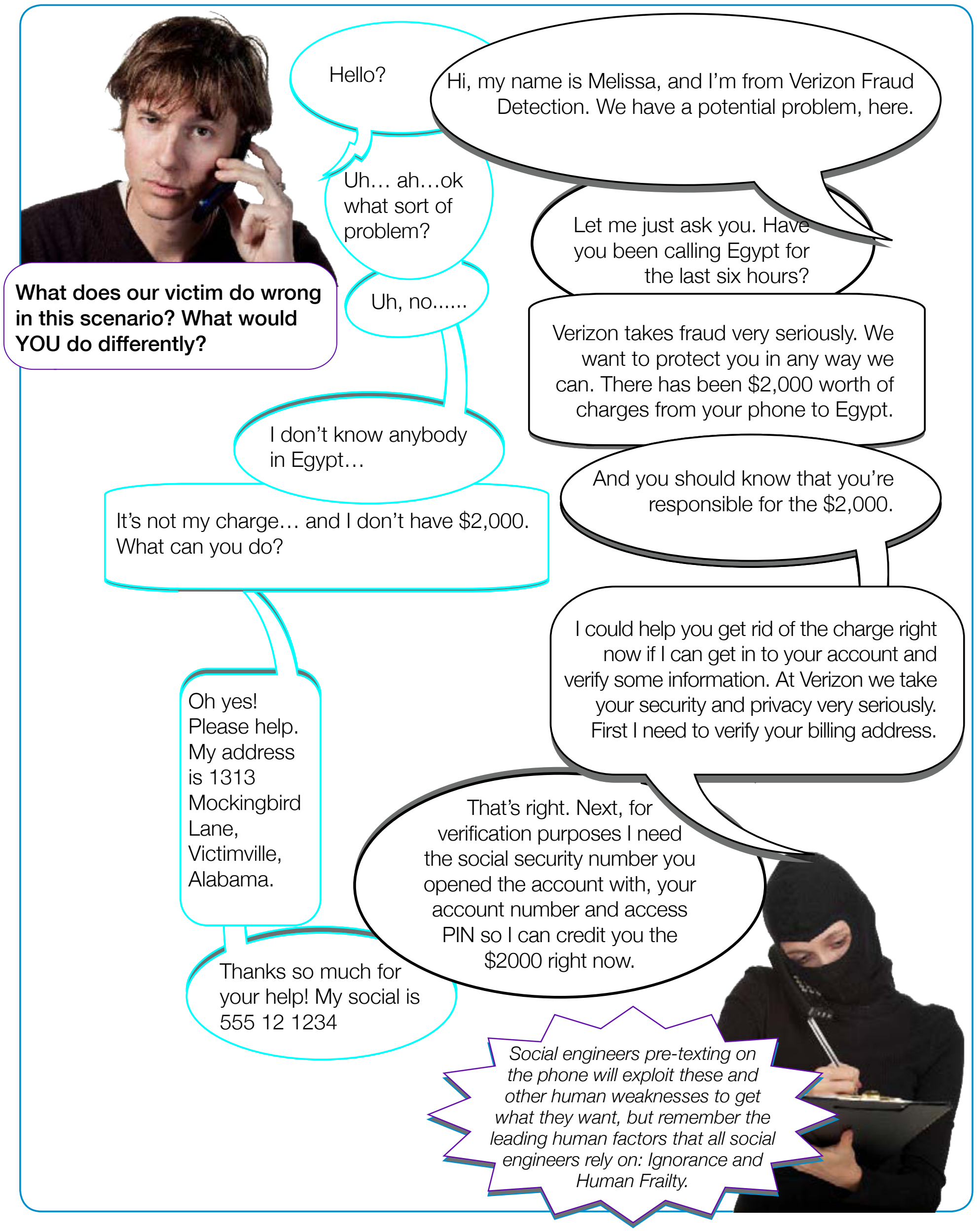
Pretexting In Action

A very common and effective form of Social Engineering over the telephone is called Pretexting. It attempts to talk people out of security relevant information.

Let's say someone calls you at home. He knows a little bit about you from his internet research and you seem like a good 'mark' or victim. The pretexter uses that info to develop initial trust. He then asks for personal or security relevant information using one of the 'motivators'.

In truth, he is just trying to con you. It is a scam and it is fraud. No matter who he says he is. Just Say No. And it's the same thing at work. If you have any suspicion at all about anyone on the telephone, just say no.

Here's an example of pretexting in action.


Hello?
Hi, my name is Melissa, and I'm from Verizon Fraud Detection. We have a potential problem, here.
Uh… ah…ok what sort of problem?
Let me just ask you. Have you been calling Egypt for the last six hours?
What does our victim do wrong in this scenario? What would YOU do differently?
Uh, no......
Verizon takes fraud very seriously. We want to protect you in any way we can. There has been $2,000 worth of charges from your phone to Egypt.
I don't know anybody in Egypt…
And you should know that you're responsible for the $2,000.
It's not my charge… and I don't have $2,000. What can you do?
I could help you get rid of the charge right now if I can get in to your account and verify some information. At Verizon we take your security and privacy very seriously. First I need to verify your billing address.
Oh yes! Please help. My address is 1313 Mockingbird Lane, Victimville, Alabama.
That's right. Next, for verification purposes I need the social security number you opened the account with, your account number and access PIN so I can credit you the $2000 right now.
Thanks so much for your help! My social is 555 12 1234
Social engineers pre-texting on the phone will exploit these and other human weaknesses to get what they want, but remember the leading human factors that all social engineers rely on: Ignorance and Human Frailty.

This pretexting example was taken from a video in our popular Social Engineering course. Click here to see more of the Social Engineering training course. (Coming soon in our Mini-Course format, as well!)

Security Awareness from A to Z

Since school is starting all around us, we thought it would be appropriate to take a look at some security ABCs, so to speak. Kids often spend the first several days of a semester 'reviewing' as their teachers get a handle on what they remember and how much they really know.

We will do the same thing for you! Your own back to school basics. A little 'review' of some security terminology across all three security domains: Cyber, Human and Physical. A handy 'cheat sheet' of terms and concepts you should know in order to be a truly security aware individual.

With that in mind, let's take a look at Security from A to Z. In fact, this handy newsletter is just the kind of security basics you, your family and friends should be aware of every day!

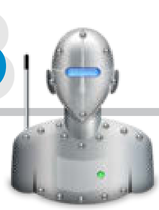
A

APT – an Advanced Persistent Threat – usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. APTs require patience, skill and resources – and can be highly effective against their victim companies.

AES is the **Advanced Encryption Standard**, which has been adopted by many governments and is used to protect data from eavesdroppers.

B

Backdoors are technical entry points into a network that many programmers install for future maintenance. Criminal hackers will often install their own backdoors to avoid detection by security software.



A **Botnet** is a collection of computers whose security has been breached. A third, unknown person, is now in control of that computer - known as a "bot". They are often used to send spam, phishing emails and conduct other online criminal actions.

C

Cybercriminals are simply criminals that use hacking and social engineering skills.

Clickjacking tricks a user into clicking on a concealed link, not the one on the screen. Users think that they are clicking visible buttons, when they are actually performing actions on the hidden page – generally very harmful to you and your computer.

D

A **DDoS Attack** is a distributed denial-of-service attack employing hundreds or thousands of computers (sometimes part of a Botnet) to target other computers, websites and/or networks and shut them down.

Dumpster Diving is looking through garbage in search of information about a company or organization, or information that can be used to help breach the company's defenses.

Data breaches cost the global economy hundreds of billions of dollars every year from stolen intellectual property, customer confidence, public image and employee PII, Personally Identifiable Information.

E

Encryption is the simplest and strongest method to protect information (both at rest and in transit) from prying eyes. Strong key management is the foundation of this powerful and essential tool.

F

FDE is **Full Disc Encryption**, an increasingly popular method for protecting the contents of laptops and other mobile devices.

Facebook and social media. Make smart posts. Your location or travel plans could be picked up by thieves. Political rants, harsh language and those 'funny' pictures can easily come back to haunt you and your online reputation. For many people, what is funny today could be a career buster tomorrow.

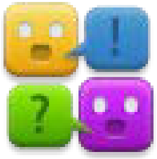
G

GLBA (Gramm–Leach–Bliley Act) is a mandatory compliance law for financial institutions. It requires that policies be in place to protect the private information of customers from foreseeable security threats.

Ghosting is a form of identity theft, where a person assumes the identity of a deceased person.

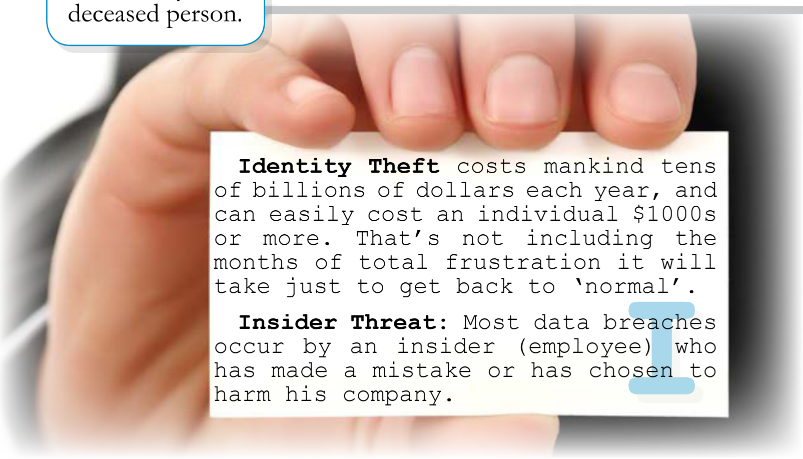
H

Hackers are people who figure out how to make computers and other technologies do more than they were originally designed to do. They are **not** criminals. Criminals who employ hacking skills are **'criminal hackers'**.



Hijacking an internet conversation or session allows the bad guy to gain unauthorized access to information or services in a computer system.

I



Identity Theft costs mankind tens of billions of dollars each year, and can easily cost an individual $1000s or more. That's not including the months of total frustration it will take just to get back to 'normal'.

Insider Threat: Most data breaches occur by an insider (employee) who has made a mistake or has chosen to harm his company.

J

Java is a popular programming language, but also has security weaknesses that have been exploited over the years. Many users turn off Java or JS (Java Script) in their browsers to minimize security risks unless specific trusted sites need it.

Jailbreaking is the intentional bypassing or removal of security and application controls built into iOS. Most workplaces do not permit jailbroken iDevices to connect to their networks. At home, only the most experienced users should experiment with jailbreaking.

K

Keys (strings of characters) are used in encryption to specify exactly how the encryption algorithm works. Symmetric keys require both parties to exchange and use the same key to encrypt and decrypt a message. With asymmetrical keys, each party uses a combination of both public and private keys.

L

Lost smartphones and laptops exceed 10,000,000 every year. Use strong passwords and FDE (Full Disc Encryption) to protect the data on lost devices.

A **Leapfrog Attack** refers to the use of a password or user ID that is obtained in one attack in order to commit another attack.

M

Maiden Names on Facebook create a security vulnerability. Security validation questions are often "What is your maiden name?" or "What is your mother's maiden name?" All it would take to break the 'code' is to know a little about your family history by looking at a social media or classmate site.

Malware is any software that causes harm to data, a computer or network. Trojan Horses, worms, spyware, viruses etc.

The **Man in the Middle Attack** is a form of eavesdropping in which the attacker makes independent connections with the victims and relays messages between them. The victims believe that they are talking directly to each other over a private connection when, in fact, the entire conversation is controlled by the attacker. This kind of attack is often associated with encryption. Web sessions with private or financial data should always be with HTTPS (the S is for secure).

Mobile devices are the first step in the *Internet of Things* (term for objects and their virtual representations). There are almost 2 billion mobile devices today, and will be more than 20 billion by 2020. The vast majority have no security controls at all.

Mouse Over is a simple technique to see what the 'real' URL or email address is in an email. Hold your mouse over the link for a few seconds and a pop up box will help you identify if you are being phished or not.

N

Netiquette is decent and proper behavior on the internet. Company policies often reflect specific netiquette to protect the company's data, networks and reputation. If you don't know the policy, it's time to find out now!

O

OSS, Open Source Software, is generally freely available (Freeware), but should be downloaded with caution because there is no oversight. Research the trust and reputation before you download any software.

OWASP, Open Web Application Security Project, is a global community effort to promote secure web (HTTP) programming.

P

Passwords are fairly weak security, but the best we have in most cases. Apply the SNL rule: Use Symbols, Numbers and Letters (UPPER and lower case) in every password you create.

Phishing emails enter our inbox every day. The goal is to scare you, make false promises or otherwise entice you to respond, give out personal information or to <click> on a link (see Mouse Over).

Pretexting occurs when a bad guy calls you on the phone, poses as someone he is not, from a company he does not represent, and tries to extract personal or security information from you. When in doubt, say nothing.

Privacy Settings on social networking sites allow you to share as little or as much information as you choose. If you do not understand how to set them properly, have a friend or colleague walk you through the basics. It is that important.

Q

QR (Quick Response) Codes are ubiquitous and handy. But the bad guys are figuring out how to make them hostile and infect your mobile devices.

R

A **Road Apple** is a malware-infected storage device, such as a USB drive. They are often left in locations to be easily found by an employee of the target company, like a parking lot, elevator or other public area. Studies have shown that the majority of people are more than happy to plug road apples into their work computer. Consequently, such attacks have the potential to be extremely effective. More notably, if the road apple is labeled with enticing words or logos (i.e., "Confidential") they are plugged in twice as often. Know and follow company policy on portable USB devices.

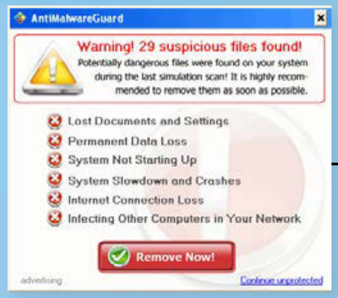
R

Reputation of websites is achieved through browsers, plug-ins and many security software packages. Know company policy and at home, avoid visiting sites that contain such warnings.

Spoofing is assuming the identity of another person. Spoofing is generally associated with hostile and/or criminal online activity.

Spam is unsolicited email, often trying to sell a product or service. A high percentage of spam is also hostile or infected with malware. Just delete spam that gets through to your inbox. At work, know and follow company policy on spam.

Social Engineering attacks the human through a variety of non-technical methods such as pre-texting, vishing, phishing and dumpster diving.



AntiMalwareGuard

Warning! 29 suspicious files found!

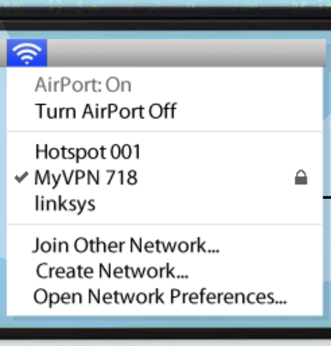
Potentially dangerous files were found on your system during the last simulation scan! It is highly recommended to remove them as soon as possible.

- Lost Documents and Settings
- Permanent Data Loss
- System Not Starting Up
- System Slowdown and Crashes
- Internet Connection Loss
- Infecting Other Computers in Your Network

Screensavers should be password protected and set to automatically turn on after a few minutes of keyboard or mouse inactivity. Know and follow company policy!

Spearphishing emails are phishing emails that target specific individuals, execs and or companies for attack.

Spyware is hostile software (malware) installed on computers that collects information about users without their knowledge. Keystroke loggers are typical examples, where every keystroke is captured and invisibly sent to a distant hostile person.



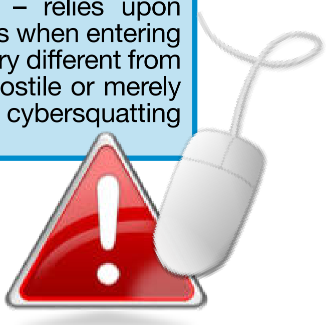
SSID (service set identification) is the broadcasted name of a wireless network. Disabling it does not really improve security, but a simple boring name may help avoid attention.

T

Tailgating occurs when a person follows you into a secure area using your credentials. Everyone should gain access only using their own badges and access mechanisms. Know and follow physical security policy at work.

A **Trojan Horse** is a type of malware that is installed on a computer without the user's knowledge. At some future date and time, the Trojan is 'turned on' and performs hostile acts against the user, the data or the computer.

Typosquatting – URL hijacking – relies upon users making typographical mistakes when entering a web address. www.Ford.com is very different from www.Frod.com and 'Frod' can be hostile or merely used for advertising. Also known as cybersquatting and brandjacking.



U

Users can be the strongest possible defense against network attacks, especially non-technical attacks like social engineering. Through awareness, common sense and cautious behavior, users can help prevent the majority of attacks against organizations.

V

Vishing is the criminal practice of using social engineering, typically over Voice over IP (VoIP) telephone services. It is most often used to gain access to private, personal and financial information from the public for the purpose of financial reward.

VPNs, **Virtual Private Networks**, create a secure means of communications between computers using encryption to scramble the information, making it unreadable to eavesdroppers.

W

WiFi (Wireless Fidelity) is also known as 802.11 communication. We use it at home, many businesses employ it and it is common at airports, hotels and other public areas. However, public and free WiFi is about as insecure as you can get. Always use a personal VPN when using any public WiFi network and follow policy with any work related devices or communication.

WPA2 is currently the minimum security standard you should use on a WiFi connection. All major wireless routers and computers have WPA2 built in.

X

XML stands for Extensible Markup Language, which is the powerful backbone language of the internet. It enhances usability, functionality and security. HTML displays the data that is managed by XML.

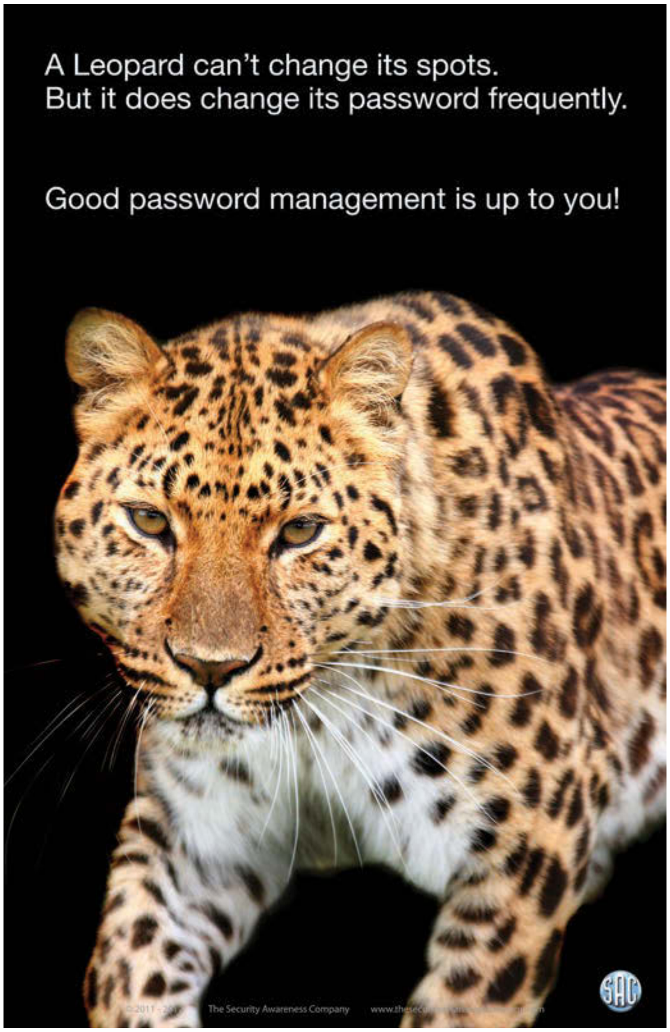
XXX (Adult-oriented) websites should never be visited at work. When at home, it's prudent to have different website access rules for different members of the family.

Y

You are the first line of defense in protecting data, computers, networks and reputation, both at work and at home. Whether you are in the building or on the road for work, common sense behavior with technology is critical to security. It is your responsibility to report any and all potential security threats you may observe.

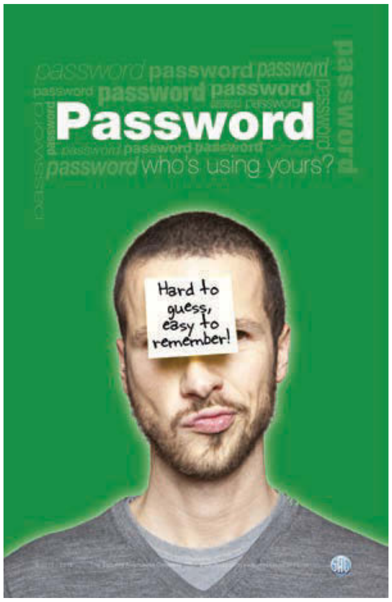
Z

Zombie. A computer which is connected to the internet and has been compromised by a criminal hacker or some form of malware. Zombies are used to perform malicious tasks of one sort or another under the remote control of 'bad guys'. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks.


A Leopard can't change its spots.
But it does change its password frequently.
Good password management is up to you!
SAC
The Security Awareness Company

GOOD PASSWORD HABITS ARE IMPORTANT TO DEVELOP AND NURTURE.

SAC's Awareness Artwork can help you do that! Yearly licenses begin as low as $50 per poster! View our entire inventory here. We have posters on every subject you could want: backup, passwords, social engineering, incident reporting, shredding, phishing, safe surfing, mobile security, confidential information, following policy, and lots more. See something we haven't covered? Let us know! Contact us today to let us help spread awareness through your office!


password password password
password password password
Password
password password password
password who's using yours?
password
Hard to guess, easy to remember!
SAC

PASSWORDS & PASSPHRASES

Make them *Easy to Remember* and *Hard to Guess!*

The longer the better.

Use UPPER and lower case letters.

Use number 0 - 9.

Use special characters #$%!!

Try the first letters of your favorite songs, movies or phrases and add a secret number!

DO NOT USE:
- names
- birthday
- pets
- any personal information that can appear on Facebook or other social networking sites

WHOOAA!
C'MON, C'MON, C'MON YOU GUYS! CHANGE MY PASSWORD! IT'S THE KEY TO OUR SECURITY AROUND HERE!

Phishing

Phishing is simply a criminal email scam with the intent to defraud. The attackers send emails that appear to be legitimate, in order to get recipients to respond and provide personal information or money. Phishing preys upon human emotions such as greed and fear, to elicit a response.

It is the most effective non-technical technique criminals use to try to bypass a company's technical controls and defenses and the leading cause of Identity Theft today.

A phishing email is the 'hook', and if you answer, you have 'taken the bait'. If you then follow along with the scam or fraud, you have been 'caught'.

Phishing is a global criminal crime wave. Tens of billions of phishing emails are sent every day to billions of users around the world. Thousands of prominent companies are 'phished' every day.

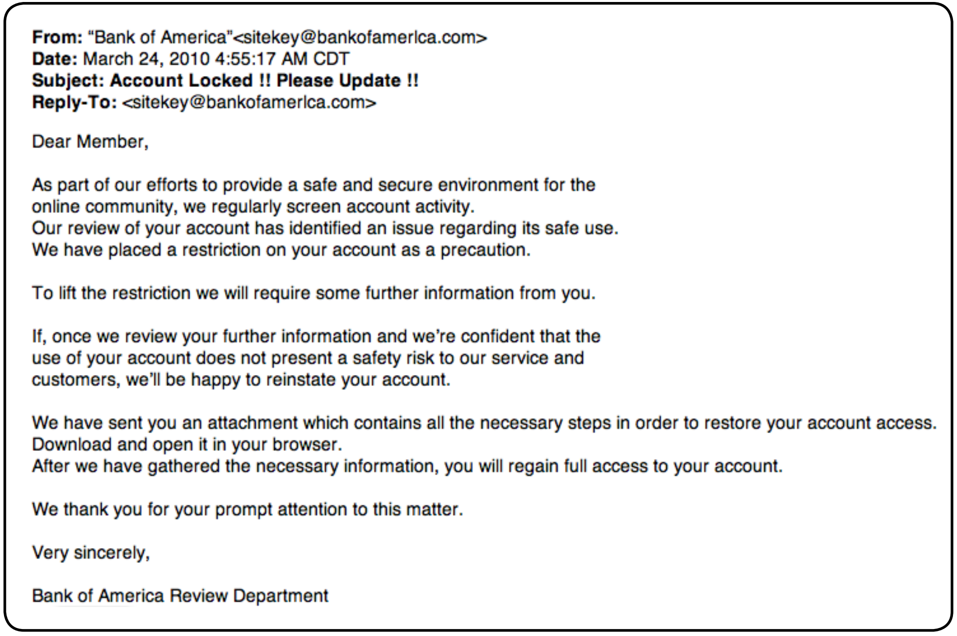
While no one knows for sure, global losses are estimated to be in the tens of billions of dollars every year… but, if you are a victim, you will almost assuredly, never get your money back. Your best defense is awareness!

71% *of phishing attacks are financially oriented.*

More than **1%** of Facebook users have already fallen for fraudulent phishing attacks. That's almost **10 million victims.**

7% of phishing attacks are from classified advertising, such as craigslist.com

What's Wrong With This Picture?



From: "Bank of America"<sitekey@bankofamerlca.com>
Date: March 24, 2010 4:55:17 AM CDT
Subject: Account Locked !! Please Update !!
Reply-To: <sitekey@bankofamerlca.com>

Dear Member,

As part of our efforts to provide a safe and secure environment for the online community, we regularly screen account activity.
Our review of your account has identified an issue regarding its safe use.
We have placed a restriction on your account as a precaution.

To lift the restriction we will require some further information from you.

If, once we review your further information and we're confident that the use of your account does not present a safety risk to our service and customers, we'll be happy to reinstate your account.

We have sent you an attachment which contains all the necessary steps in order to restore your account access.
Download and open it in your browser.
After we have gathered the necessary information, you will regain full access to your account.

We thank you for your prompt attention to this matter.

Very sincerely,

Bank of America Review Department

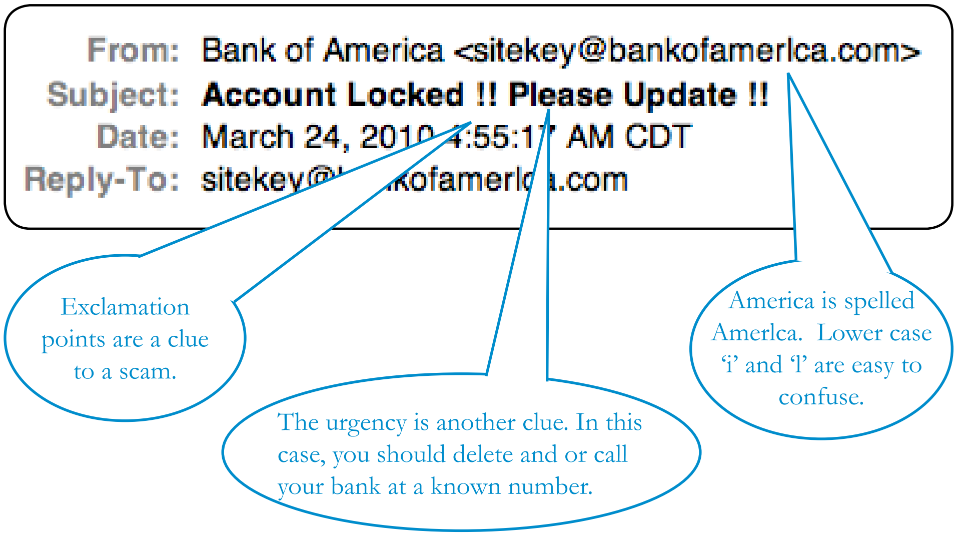
One of our colleagues received an email with this 'header' on his laptop. The body warned him about an irregularity in his account that needed immediate attention.

To make sure it was real, he looked carefully at the email address and noticed there was even an Abuse Reporting email address for the bank. (The attackers used a Sitekey email address for the bank. Sitekey is a real product - an added layer of security many financial sites use to prevent customer fraud.)

Is this a legitimate email from Bank of America? If yes, how can you tell? If not, how do you know?

Answer on the following page.

What's Wrong? Answer!



From: Bank of America <sitekey@bankofamerlca.com>
Subject: Account Locked !! Please Update !!
Date: March 24, 2010 4:55:17 AM CDT
Reply-To: sitekey@bankofamerlca.com

Exclamation points are a clue to a scam.
The urgency is another clue. In this case, you should delete and or call your bank at a known number.
America is spelled Amerlca. Lower case 'i' and 'l' are easy to confuse.

Craigslist Scam

Another colleague was selling a chess set on her local Craigslist. She was inundated with emails asking if she could ship it right away. "Yes, I can". She started getting checks in the mail for up to ten times the price she asked for the chess set.

The scam is simple. The buyers ask the victim to cash the check at a 'Check Cashing Office' right away to establish trust. They also ask for the victim, to send some of it back via Western Union for their 'accidental overpayment'.

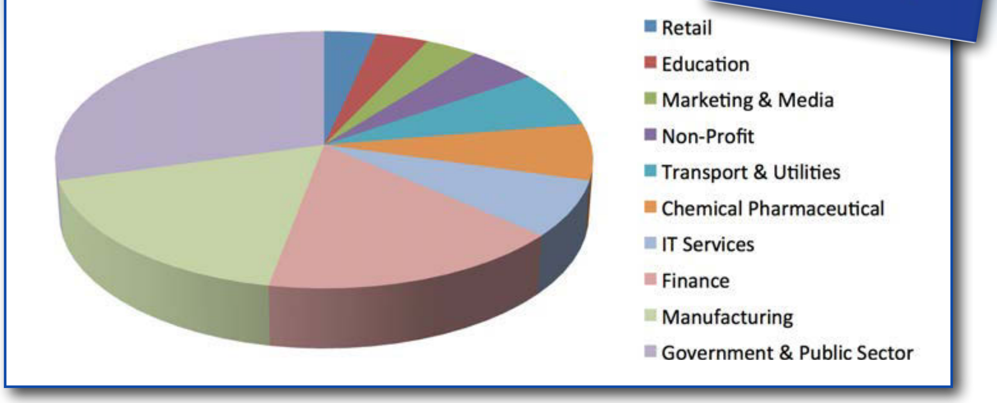
Malware is No Longer a Rising Tide
Today, it's a Global *Tsunami*!

Quick Quiz

How many unique types and variants of malware are there on the internet?

- □ 10M
- □ 1,000
- □ 1Billion
- □ 10,000
- □ 400M
- □ 100,000
- □ 100M
- □ 600M

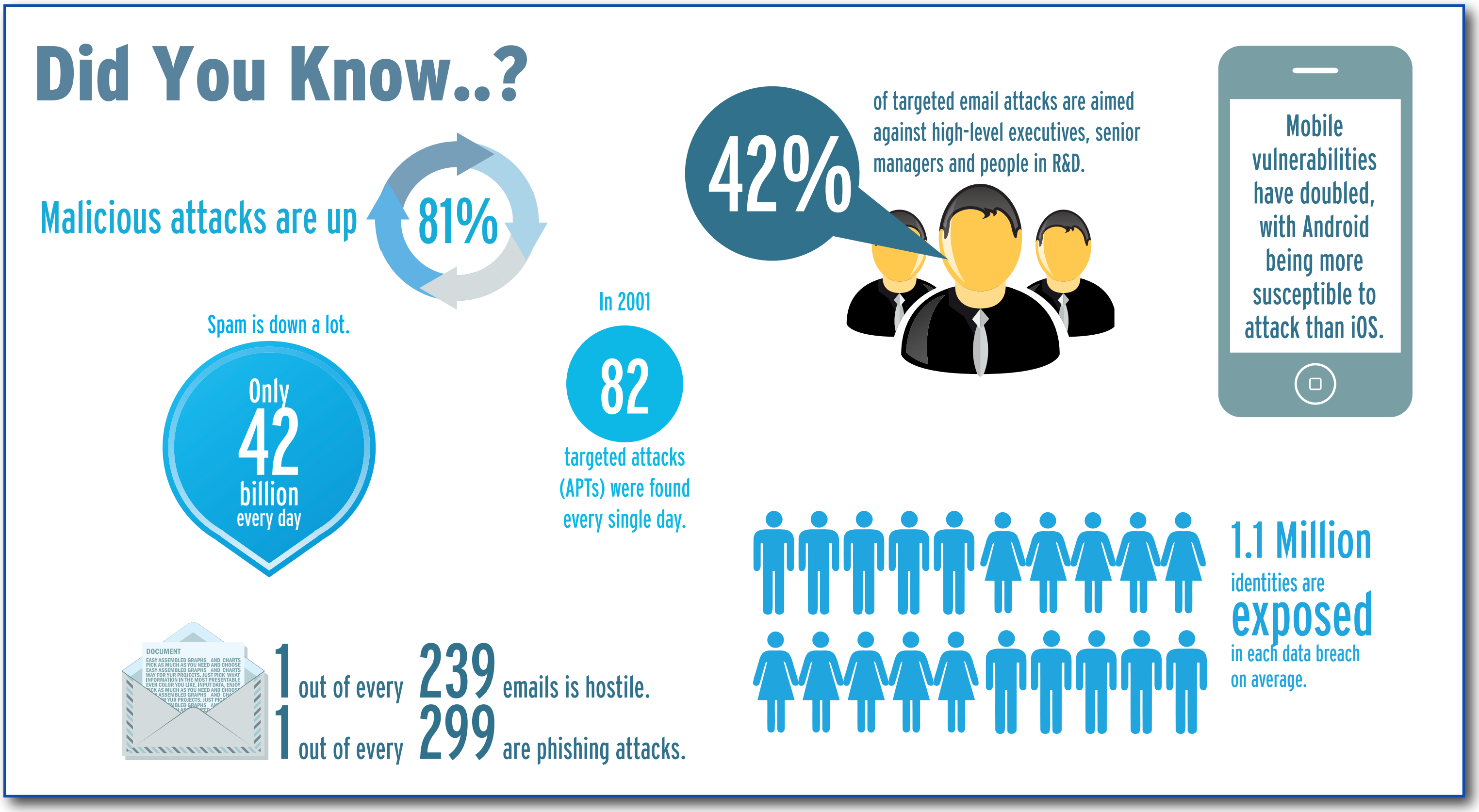
Targeted Email Attacks by Sectors, 2011



Between APTs (Advanced Persistent Threats) from organized crime to nation states and huge financial and manpower investments in cybercrime, malware is everywhere.

The numbers speak for themselves and should tell you why we care so much about using proper internet behavior, emailing with care and browsing more carefully than ever before.

Did You Know..?



Malicious attacks are up 81%

Spam is down a lot.

Only 42 billion every day

In 2001

82 targeted attacks (APTs) were found every single day.

42% of targeted email attacks are aimed against high-level executives, senior managers and people in R&D.

Mobile vulnerabilities have doubled, with Android being more susceptible to attack than iOS.

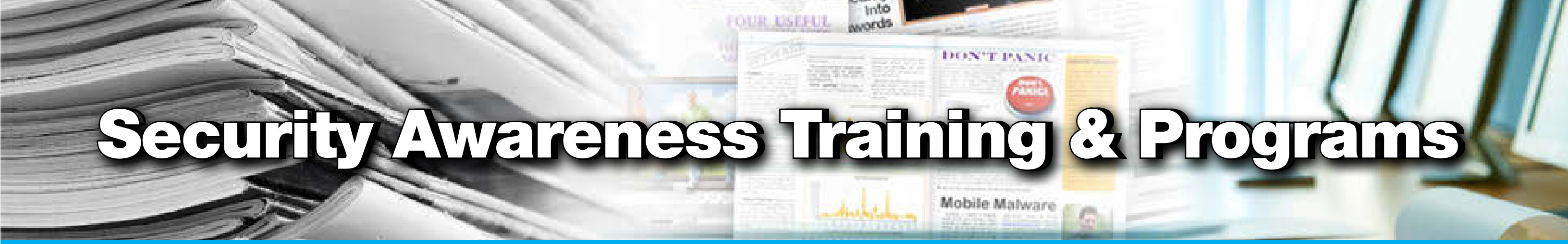
1 out of every 239 emails is hostile.

1 out of every 299 are phishing attacks.

1.1 Million identities are exposed in each data breach on average.

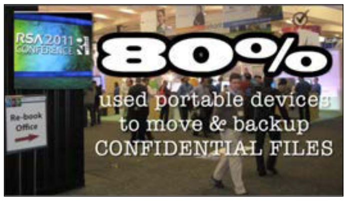
Quick Quiz Answer: More than 600 million variants of malware have been identified, with current identification at more than 30 million new ones every month. Yes, that's million. By the end of 2012, the number is expected to approach 700 million unique malware variants.

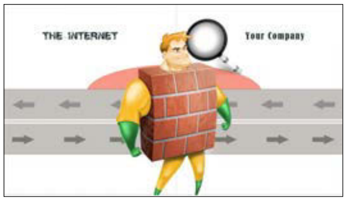
Security Awareness Training & Programs



If you can change behavior, you can achieve better security.

THREE-QUARTERS OF INCIDENTS INVOLVING LOSS OF SENSITIVE DATA ARE CAUSED BY FAILURE & HUMAN ERROR.





Engaging, Interactive Multi-Media Courses branded for your entire organization:

- Most courses are available in SCORM/AICC, Server, Web, CD and Video streaming formats with branding and specific user navigation options.
- SA 101
- The Human Firewall
- Social Engineering
- Mobile Security
- Industry Specific & ANSI-Approved Compliance Modules including HIPAA, PCI and ISO-17799
- Assessments & Metrics
- Learning Games & Quizzes
- Hosted or non-hosted

Add the following branded, unbranded or custom components to your existing SA Program:

Monthly Awareness Newsletters

Security Awareness Logo / Mascot Designs

Security Awareness Video messages

Security Awareness Art & Calendars

Security Awareness Days, Webinars or Executive Briefings

information security
Don't Panic! Tips and Tricks to Keep Your Computer Clean
TINYURL: COOL TOOL OR WEAPON OF EVIL?
THE MAN FACE
Mobile Malware
security awareness n
Understanding the Cyber Domain
Physical Security and YOU!
Securing the Human Domain
information security news
July 2011
FREE WiFi: Can You Afford It? How using free, unsecured networks can be dangerous.
What is a VPN? How Virtual Private Networks keep you safe in cyberspace.
Choosing a VPN A few suggestions to help you make the choice.
The Trouble with Travel Keeping your mobile devices safe while traveling.
COOL MOBILE ENTERPRISE SECURITY TOOL

Changing Behavior One <CLICK> at a Time

For more information and to see demos of our courses, visit our website or contact us directly at 727.393.6600

www.TheSecurityAwarenessCompany.com