information security **top 10** for managers

"Security" can mean protecting money and valuables by using locks on doors, bars on windows, and guards to keep bad guys out. **Information Security** means protecting not *things*, but *information*: credit card numbers, passwords, and personal information that criminals use to steal money, access confidential data, or just cause harm to people and companies because they can. How do they get that information? Email, texts, your customers' credit cards, and more. In your workplace, information criminals want shows up in several ways and places. Information Security is the responsibility of every employee.

The following 10 tips are simple things that you, as a manager, can do to protect information in your workplace.

be aware

1. Be aware of **laws and regulations** that affect the types of information you work with.
2. Stay up-to-date on **security threats** that affect your industry.
3. Educate your employees on information security **best practices**: security is a team effort.
4. Keep software up-to-date with the most current **anti-virus software and security patches**.

be secure

5. Never share **passwords or login information** with anyone, not even coworkers.
6. Never write down customer **credit card information**, or take a card out of the customer's sight.
7. Store **hard copy data** (information on paper, or not stored electronically) in a safe and secure location.

friend or foe?

8. Only click **links in emails** sent from trustworthy sources.
9. Check that **visitors** *(repair technicians, vendors, etc.)* are who they say they are before giving access to secure areas, cash registers, or other points of sale.
10. **Manage employees** to make sure credit card and other information is handled with information security best practices every day.

I acknowledge with my signature that I have read **information security top 10 for managers** and understand that Information Security is the responsibility of every employee.

Name: _____ Date: _____

information security basics

SIMPLE ACTIONS PREVENT REAL RISKS

The truth is, YOU are the most important defense your company has against criminals out to steal information. No matter what your role in the company, you are #1 in security defense. That's why security awareness is so important. Things you may typically think of as harmless, such as clicking on a link in an email or sharing passwords, may put valuable information at risk. On the following pages you will learn:

- How seemingly innocent actions can put the security of your company at risk.
- What criminals want to steal, and why.
- The best ways to help keep information safe.

SECURITY AWARENESS

Your Job

It's the responsibility of every employee to be security-aware and to use best practices every day. So, what is security awareness?

SECURITY AWARENESS	WHAT TO DO	SEE SOMETHING, SAY SOMETHING	BECOME FAMILIAR
Security awareness means having the knowledge and attitude to protect information. Be aware of the potential for information to be misused or stolen, and recognize the actions you can take to protect the security of your company and customers.	Learn the basics of security awareness on the pages that follow. Follow best practices, and help your employees to do so as well. Simple things like not sharing passwords and keeping doors locked can make a big difference in information security.	You can also help by recognizing and reporting security risks you observe. For example, if an unscheduled maintenance person shows up, it's your job to make sure they are who they say they are.	Review the information on these pages carefully to learn what to look out for and how to respond. You should also become familiar with your company's security policy and the preferred way to report security risks.

What's Next?

Now that you have an understanding of security awareness and your role, what's next?

- Complete all the recommended training for your job.
- Become familiar with your organization's security policies and procedures.
- Use the best practices you learn every day.

stealing information

WHAT ARE CRIMINALS AFTER?

Information security criminals want to steal information. Sometimes, they use the information to steal or scam money. Sometimes, they sell the information to others. And in other cases, stolen information may be used as a stepping stone to a bigger target: for example, a stolen password may not seem like such a big deal, but it can lead to access to a manager's office and the information inside. In 2012, the most popular target was credit card information.

Not all information criminals are looking for financial profit. For example, a list of email addresses may be used to help hackers spread a virus. We can't always guess how information might be used by a criminal, so we need to protect it at all times. Recognizing that criminals are out there and want to steal information, the best defense is to keep a close eye on all information, no matter how seemingly small.

What to Keep Private?

There are all kinds of information that should be kept private and secure. Your company may even have a policy on how you should treat the different types of information you work with each day. Find out if your company has rules about how to handle sensitive information. Below are examples of information that should be kept private and secure.

Credit Card Numbers

Personal Information (phone and identification numbers, addresses, etc.)

Internal Company Information (policies, product information)

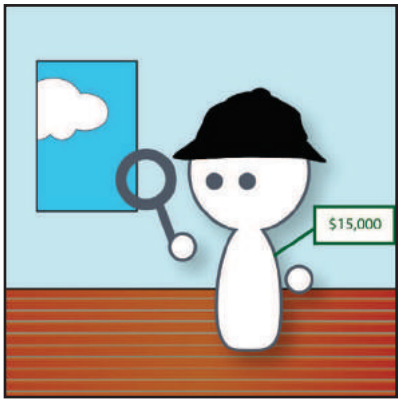
Passwords

WHAT'S THE BIG DEAL?

Stolen information is a very big deal. When it happens to a company, called a "**breach**," the damage to victims can be huge. In 2012, nearly every industry, country, and type of information was involved in security breaches of some kind. Below are a few examples of the damage YOU can prevent.

Loss of customer information can cause companies to **lose customers, damage their reputation and ruin relationships** with business partners.

Companies may be required to pay **large fines** and fees if the stolen information is confidential, such as credit card numbers or personally identifiable information (PII).



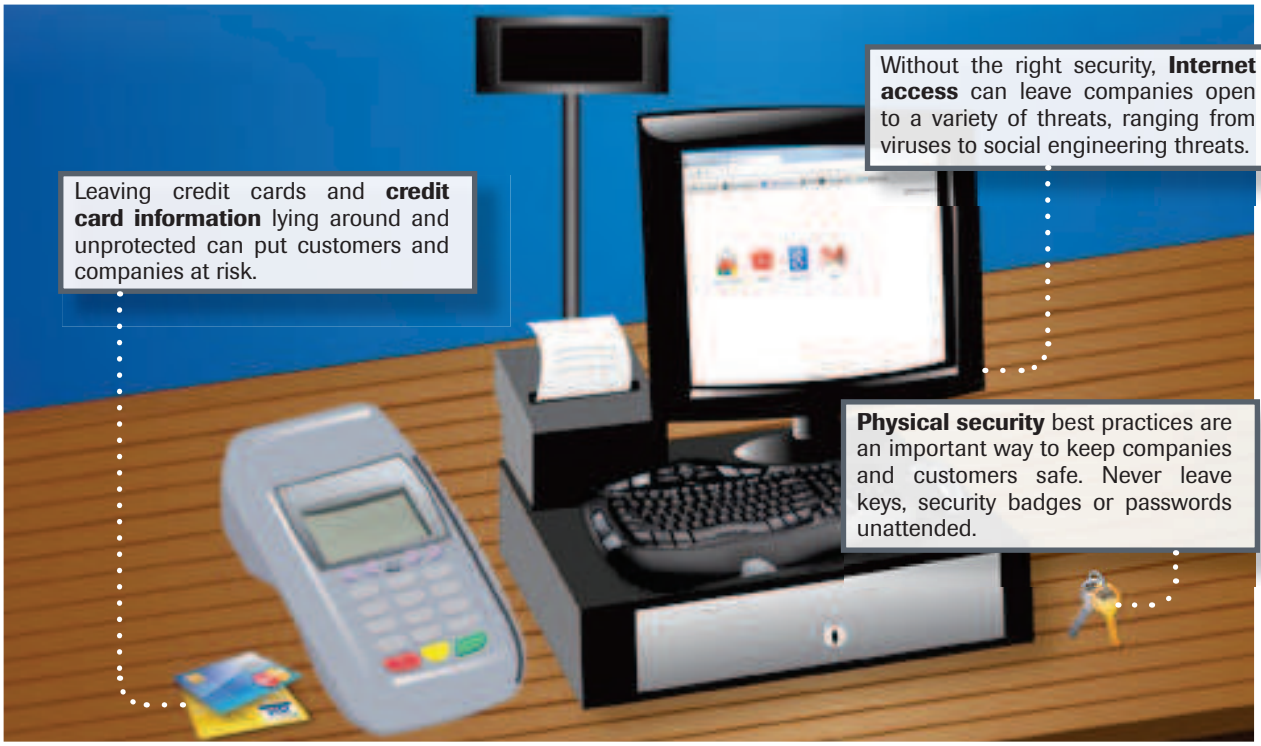
If a breach occurs, your company may be required to undergo an **investigation**. Investigations are expensive, starting around $15,000.

The bottom line: A lot is at stake when it comes to information. Losing information or suffering an attack can be enough to put some businesses **out of business**. In 2011, 39% of data lost was caused by **employee actions**. As a manager, it is critical you understand your role in information security.

danger zones

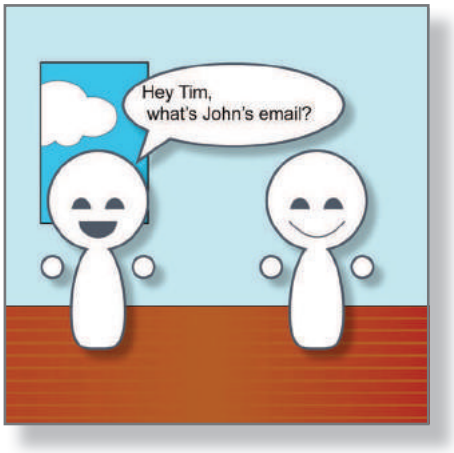
Information Everywhere

Below is an example retail workspace. Take a look at the types of information we are surrounded by and need to protect daily.



Stranger Danger

Before sharing information with others, consider both the information type and how it could be used. The example below shows two different scenarios: the first one safe, the second one unsafe.



Sharing a coworker's email address with a fellow employee is a harmless action many people do regularly on the job.

Sharing the same information with an unidentified caller could lead to trouble: malware, stolen personal information or even a company-wide security breach

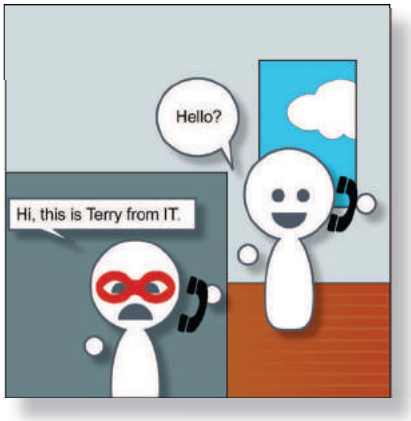
Remember, information that is fine to share with coworkers may not be okay to share with strangers, customers, or vendors. Think twice about requests over the phone, in email, or in person, and make sure you are certain the person is safe to share information with.

social engineering

WHO ARE "SOCIAL ENGINEERS"?

A person who **tricks another person** into giving access or information is a social engineer. They're sometimes called hackers, fraudsters, hoaxers, swindlers, or imposters, and they'll use email, phone calls, or in-person visits to trick you into giving out information you shouldn't. Most attempts to steal information or pull off scams involve social engineering.

Social engineering relies on *people* to be the weak link in the security chain: That means YOU. Social engineers use humans, not technical hacking techniques, to help carry out their attacks.



Rather than using software to steal your password, a social engineer may call you pretending to be a member of your organization's IT staff and simply ask you for the information they need.

Rather than trying to get around your company's security systems to install harmful software on your computer, a social engineer may send you an email designed to trick you into clicking a web link that does their dirty work for them. This is often called "phishing."

Rather than hacking a store's point of sale system to get access to customer credit card numbers, a social engineer may pose as a repair person who needs access to your store's system.

TARGETS OF SOCIAL ENGINEERING

Anyone can be a target of social engineering. It's easy for you or your employees to put your company and personal information at risk through a lack of awareness.

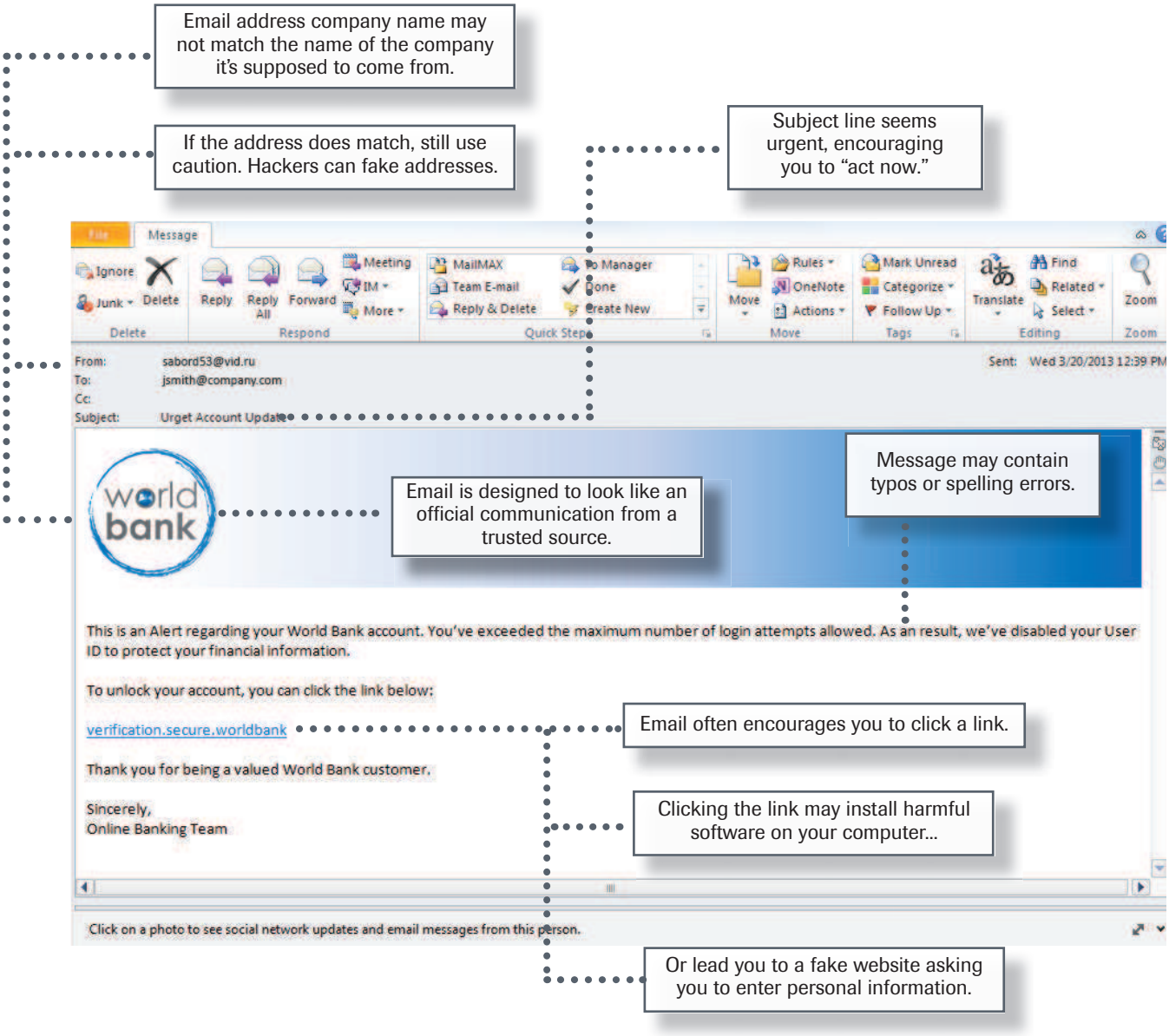
You may be thinking, "Even though I have valuable personal information, like my social security number and credit card numbers, I don't have access to any confidential information at work. **I doubt a social engineer would target me**."

Don't be so sure. Remember that we can't always guess what a social engineer is after, or how information might be used. Even if information seems harmless and is not confidential, like email addresses or phone numbers, it still needs to be protected.

The bottom line: Social engineers have a variety of goals and anyone -- you or your employees -- could be a target to help them complete their scam. Always check the identity of a person asking for access to physical locations, systems, or information. Make sure they have a business need and permission to have the information or access they are requesting. *If you are ever unsure whether you should provide someone with information or access to your company, don't.*

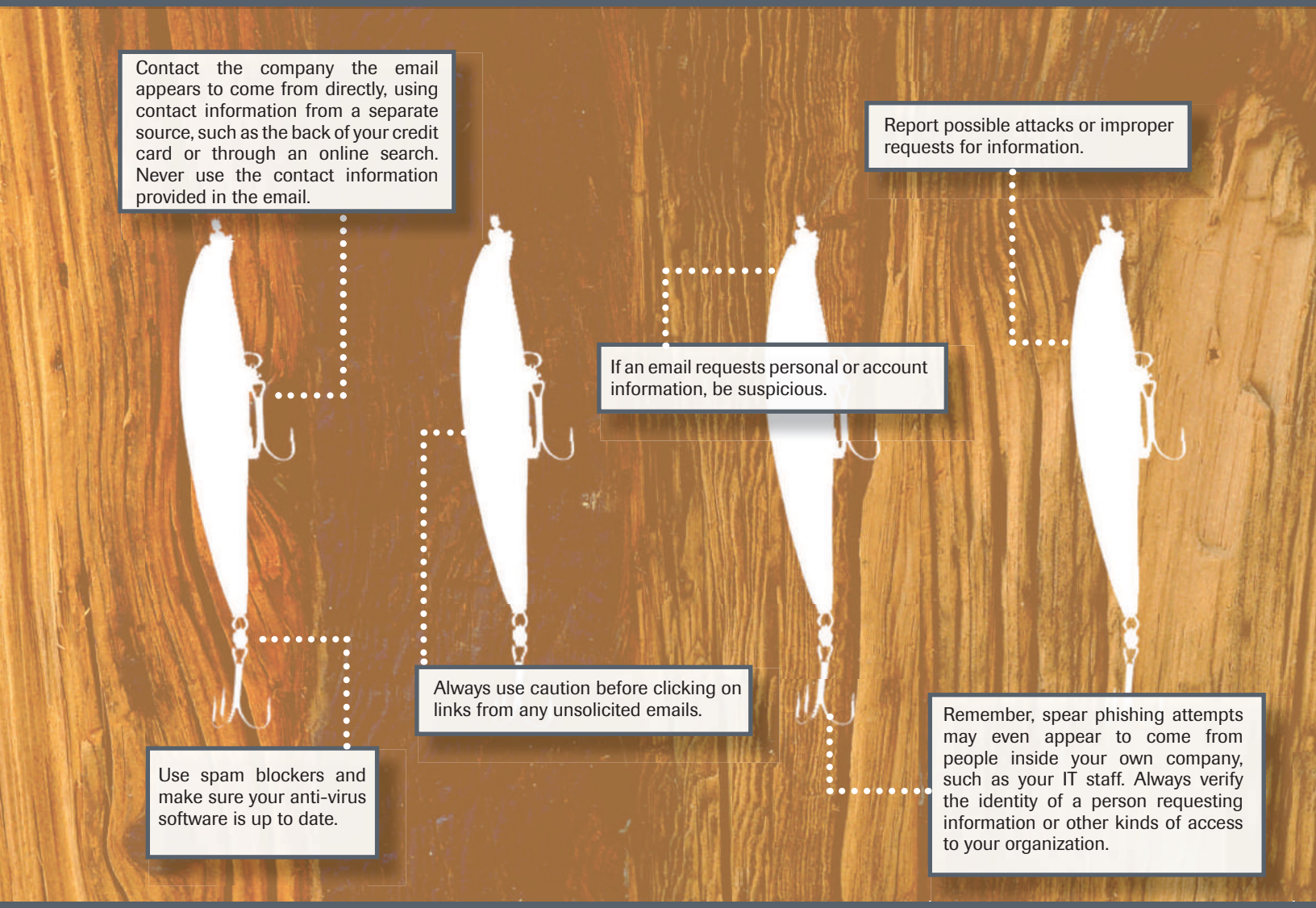
anatomy of a phish

Phishing is a popular email ploy to trick you into providing sensitive information by disguising emails to look like they are from a legitimate, trustworthy source. See the image below to learn common characteristics of a phishing email.



Some phishing attempts send out a lot of emails in hopes of someone clicking on the links they contain. Other times, the emails are more targeted and sent to specific people who have a greater likelihood of being tricked, called **spear phishing**. Spear phishing emails are well-crafted and can look very real.

catching a phish



DON'T BECOME A TARGET

The following tips can help reduce the risk of being a target of phishing:

- Never use your business or primary personal email address to sign up for websites or other non-essential Web services.
- If your email address is not required to sign up for a service, don't provide it.
- Create an alternate email address specifically for website registration and mailing lists.

a manager's role

SECURITY AWARENESS FOR MANAGERS

As a manager or owner it is your responsibility to keep your company and customer information safe. You and your employees are the most important defense your organization has against hackers and other criminals out to steal valuable information. That's why security awareness education is so important. Things you may think of as harmless, such as clicking on a link in an email or sharing passwords, may put valuable information at risk. Being trained in security awareness is the first step to keeping your organization and your customer's information safe. On the following pages you will learn:

- Security awareness responsibilities of retail managers and owners.
- Laws, regulations, methods and best practices that help keep information safe in a retail environment.
- How to guard sensitive information and maintain security.

A Manager's Responsibility

Keeping information secure is a team effort, and as leader of the team it is your responsibility to be aware of the laws and regulations that affect the information you work with. We discussed earlier the importance of knowing your company's policies and procedures. Along with those polices and procedures, you should also be familiar with laws and regulations that impact the information you work with. The following are the most common security regulations:

PCIDSS	STATE PRIVACY LAWS	SARBANES-OXLEY (SOX)
The Payment Card Industry Data Security Standard (PCIDSS) is a set of twelve standards made to protect cardholder data.	Most states in the US have privacy laws in place to protect citizens' personal information. These laws require protection of sensitive information like social security numbers, tax records, insurance records and employment records.	SOX was passed in 2001 and requires publicly-traded companies in the U.S. to have internal controls over the financial reporting process, which includes controls over the information systems that store financial data.

Knowing the different rules and regulations that affect your company's security is an important step in keeping information secure. Along with the rules and regulations, you should also be aware of the best practices that help protect companies from becoming victims:

Best Practices:

- Security threats are ever changing and evolving. Being aware of and on the lookout for common information security threats will go a long way towards keeping your sensitive information protected.
- Make sure your Point of Sale (POS) system and any hard copy data are kept safe.
- Manage the security of vendor products that your business uses. You will learn more about how to manage your vendors later on in this pamphlet.
- Train your employees on security awareness and how to maintain the security of your business.

protecting information

Knowing how to protect information goes a long way to preventing a breach at your company. Learn the following information, share it with your employees, and maintain best practices.

Security Threats

The number one way to protect your company is to be aware of information security threats and take measures to avoid becoming a victim. It is important to remember that information security threats come in all shapes and sizes. Poor security controls, software weakness, false identity, and employee theft are common; below are examples of each.

Poor Security Controls
A restaurant has five cash registers supported by a third-party service provider. The provider uses remote connection software to connect to the registers for troubleshooting and maintenance. The software is set up to accept calls 24/7 from any number and does not require a password to connect. In this situation, a data thief can easily access one or all of the registers and install software that will send them customer card data every time a credit card is swiped.

Software Weakness
A company has created an e-commerce website, but the software is poorly coded to handle credit card transactions. In this situation, a data thief can easily take advantage of this weakness and copy card data directly from the website.

False Identity
A "repair technician" picks up a card swipe terminal for repairs, without showing ID. The store terminal is taken away for service and a temporary replacement card reader is left in its place. In this situation, the temporary card reader that was left in the store may be hacked to copy credit card data. When the technician returns to pick it up, they could easily walk away with all the cardholder data captured by the machine.

Employee Theft
An employee takes a customer's credit card out of the customer's sight, either behind a counter or to a back room. In this situation, the employee could easily copy the cardholder data or even run the card through an illegal card reader to capture the customer's card information.

Keep Hard Copy Data Safe

In a retail environment you probably deal with hard copy data every day. Reports, receipts and other forms of hard copy data you handle each day may contain sensitive information, and should always be protected. The following methods will help keep your hard copy data private:

- Store hard copy information containing cardholder data in a secure and locked location.
- Check stored hard copy data regularly to make sure nothing has been tampered with or stolen.
- Make sure cardholder data is stored on paper only when absolutely necessary.
- Destroy any hard copy data that is no longer needed by using a cross-cut paper shredder or other secure method.

Manage Vendors

Many organizations use vendors to install and maintain their important systems, such as the point of sale system and firewalls. As a result, vendors are often given special access to systems that store, process and transmit sensitive data, like cardholder information.

Even if you have outsourced business responsibilities to a vendor, you are still accountable for the security of your data. Be sure to understand which security requirements your vendor is meeting and check that they are in compliance with the PCI DSS and other laws and rules that apply to you. Your vendors are required to meet Payment Card Industry standards, and you are required to have contractual language in place that states this.

Train Associates

As a business owner or manager, you are **required** to make sure that all your employees that come into contact with cardholder data are trained on Security Awareness. You must train your employees when they are hired, and provide them follow-up training once a year. You should also maintain security awareness throughout the year by using simple reminder methods such as posters, meetings and quarterly emails.

point of sale (POS)

Protect Your Point of Sale

Point of sale systems are an important part of the cardholder data flow, and they must be protected from security threats. What can you do to make sure your point of sale systems are protected?

a) Install a Firewall: Installing a firewall helps to stop people from entering, exiting, or viewing your system without your knowledge or permission.

b) Install Additional Software:

- File Integrity Monitoring (FIM) adds an extra layer of protection against unauthorized changes to your system.
- Install an Intrusion Detection or Prevention System - IDS/IPS sensors help to find and stop unwanted network traffic.

c) Apply Security Patches: Security patches are made to fix security vulnerabilities in software and operating systems. Be sure yours are up to date.

d) Be Familiar with your POS Vendor's Security Measures: It is never safe to assume that your vendor is taking care of your security requirements. Make sure your vendors show proof that they use secure practices.

Maintain Security

Security awareness is an ongoing process for managers and employees. Keep up-to-date with industry standards, regulations, and best practices. Create a security awareness plan and put it into action today!

seguridad de la información, las **10 principales** medidas para gerentes

"Seguridad" puede significar proteger el dinero y los objetos de valor mediante la utilización de cerraduras en las puertas, barrotes en las ventanas y guardias que les impidan el ingreso a los malhechores. **Seguridad de la información** no significa proteger cosas, sino información: números de tarjetas de crédito, contraseñas e información personal que los delincuentes pueden utilizar para robar dinero, acceder a datos confidenciales o simplemente causarles daño a personas o a compañías, por el hecho de poder hacerlo. ¿Cómo obtienen la información? A través de mensajes de correo electrónico o de texto, tarjetas de crédito de sus clientes y de muchas maneras más. En su trabajo, la información que los delincuentes desean aparece en diferentes maneras y lugares. La seguridad de la información es responsabilidad de todos los empleados.

Los 10 consejos a continuación son cosas simples que usted, como gerente, puede hacer para proteger la información en su trabajo.

esté atento

1. Esté atento a las **leyes y normas** que afectan los tipos de información con los que trabaja.
2. Manténgase actualizado sobre las **amenazas a la seguridad** que afectan a su industria.
3. Capacite a sus empleados sobre las **mejores prácticas** de seguridad de la información: la seguridad es un trabajo en equipo.
4. Mantenga actualizado **el software con el software antivirus y las revisiones de seguridad** más recientes.

manténgase seguro

5. Nunca comparta sus **contraseñas o información de inicio de sesión** con nadie; ni siquiera con compañeros de trabajo.
6. Nunca escriba **información sobre la tarjeta de crédito de su cliente** ni aleje la tarjeta de la vista del cliente.
7. Guarde los **datos impresos** (información en papel; aquella que no se guarda de manera electrónica) en un lugar seguro y protegido.

¿amigo o enemigo?

8. Solo haga clic en vínculos dentro de correos electrónicos que reciba de fuentes confiables.
9. Verifique que los **visitantes** *(técnicos de reparación, proveedores, etc.)* sean las personas que dicen ser antes de darles acceso a las áreas seguras, cajas registradoras u otros puntos de venta.
10. **Administre a los empleados** para asegurarse de que la información relacionada con las tarjetas de crédito y otro tipo de información se maneje a diario con las mejores prácticas de seguridad de la información.

Al firmar, acepto que leí **seguridad de la información, las 10 principales medidas para gerentes** y que comprendo que la seguridad de la información es responsabilidad de todos los empleados.

Nombre: _____ Fecha: _____

principios básicos de seguridad de la información

ACCIONES SENCILLAS EVITAN RIESGOS REALES

La verdad es que USTED es la defensa más importante de su compañía contra los delincuentes que buscan robar información. No importa qué función cumpla en la compañía; usted es la 1ra defensa en seguridad. Por eso es tan importante la concienciación sobre seguridad. Las cosas que comúnmente pueden parecerle inofensivas, como hacer clic en el hipervínculo de un correo electrónico o compartir contraseñas, pueden poner en riesgo información valiosa.
En las siguientes páginas aprenderá:

- Cómo las acciones que parecen no ocasionar daño alguno pueden poner en riesgo a su compañía.
- Qué desean robar los delincuentes y por qué.
- Las mejores maneras de ayudar a mantener la información a salvo.

CONCIENCIACIÓN SOBRE SEGURIDAD

Su deber

Es responsabilidad de todos los empleados estar conscientes de la seguridad y utilizar las mejores prácticas a diario. Entonces, ¿qué es la concienciación sobre seguridad?

CONCIENCIACIÓN SOBRE SEGURIDAD	QUÉ HACER	SI OBSERVA ALGO, DIGA ALGO	FAMILIARÍCESE
Concienciación sobre seguridad significa contar con el conocimiento y la actitud para proteger la información. Esté atento al posible uso indebido o robo de la información y reconozca las medidas que puede tomar para proteger la seguridad de la compañía y de sus clientes.	Aprenda los principios básicos de la concienciación sobre seguridad en las páginas que se encuentran a continuación. Siga las mejores prácticas de seguridad y ayude a sus empleados a que también las sigan. Cosas simples como no compartir contraseñas y mantener las puertas cerradas con llave pueden hacer una gran diferencia en lo que se refiere a la seguridad de la información.	También puede ayudar si reconoce e informa los riesgos de seguridad que observa. Por ejemplo, si una persona de mantenimiento hace una visita no programada, su deber es asegurarse de que esa persona sea quien dice ser.	Revise la información de estas páginas con cuidado para aprender a qué debe estar atento y cómo reaccionar. También debe familiarizarse con la política de seguridad de su compañía y la forma preferida para informar sobre los riesgos de seguridad.

¿Qué sigue?
Ahora que sabe de qué se trata la concienciación sobre seguridad y cuál es su función, ¿qué sigue?

- Realice toda la capacitación recomendada para su trabajo.
- Familiarícese con las políticas y los procedimientos de seguridad de su organización.
- Utilice a diario las mejores prácticas que aprenda.

robo de información

¿QUÉ BUSCAN LOS DELINCUENTES?

Los delincuentes de seguridad de la información quieren robar información. A veces, utilizan la información para robos o estafas de dinero. Otras veces venden la información a terceros. Y en otros casos, la información robada puede utilizarse como un peldaño para alcanzar un objetivo más grande: por ejemplo, es posible que una contraseña robada no parezca algo grave, pero puede que sirva de acceso a la oficina de un gerente y a la información que se encuentre allí. En 2012, el blanco más popular fue la información de tarjetas de crédito.

No todos los delincuentes que roban información buscan obtener ganancias financieras. Por ejemplo, una lista de direcciones de correo electrónico se puede utilizar para ayudar a los piratas informáticos a difundir un virus. No siempre podemos adivinar cómo utilizará la información el delincuente, por lo que necesitamos protegerla en todo momento. Dado que los delincuentes acechan y quieren robar la información, la mejor defensa es estar atento a toda la información, sin importar lo insignificante que pueda parecer.

¿Qué se debe mantener en privado?

Existen muchos tipos de información que debe mantenerse segura y privada. Su compañía puede incluso contar con una política sobre cómo debe tratar los diferentes tipos de información con los que trabaja a diario. Averigüe si su compañía tiene reglas respecto al manejo de la información confidencial. A continuación se muestran ejemplos de información que debe mantenerse segura y privada.

Números de tarjetas de crédito

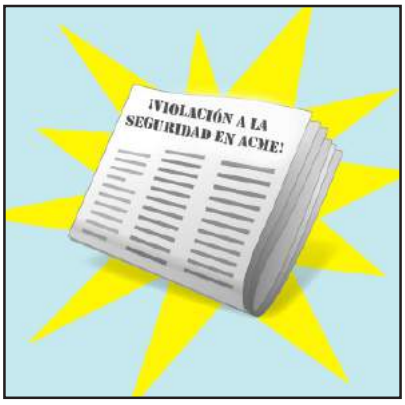
Información personal (número de teléfono, número de identificación, direcciones, etc.)

Información interna de la compañía (políticas, información de los productos)

Contraseñas

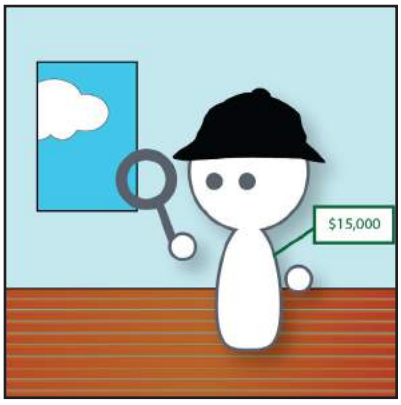
¿CUÁL ES EL PROBLEMA?

El robo de información es un gran problema. Cuando esto ocurre en una compañía, denominado "**violación**", el daño a las víctimas puede ser enorme. En 2012, casi todas las industrias, los países y los tipos de información sufrieron algún tipo de violación de la seguridad. A continuación se muestran algunos ejemplos del daño que USTED puede evitar.



La pérdida de la información del cliente puede hacer que las compañías **pierdan clientes, puede dañar su reputación** y arruinar las relaciones con los socios comerciales.

Es posible que las compañías deban pagar **importantes multas** y honorarios en el caso de que la información que se haya robado sea confidencial, como cuando se trata de números de tarjetas de crédito o información de identificación personal (PII).



Si se produce una violación, es posible que su compañía deba someterse a una **investigación**. Las investigaciones son costosas, desde $15,000.

Conclusión: hay mucho en riesgo cuando se trata de información. Perder información o sufrir un ataque puede ser motivo suficiente **para cerrar** algunas empresas. En 2011, el 39 % de los datos perdidos se produjo por **acciones de los empleados**. Como gerente, es fundamental que entienda su función en la seguridad de la información.

zonas peligrosas

Información por todas partes

A continuación se muestra un ejemplo del lugar de trabajo de un minorista. Observe los tipos de información que nos rodean y que deben protegerse a diario.

Peligro de desconocidos

Antes de compartir la información con otros, tenga en cuenta el tipo de información y cómo se podría utilizar. El ejemplo que se encuentra a continuación muestra dos situaciones distintas: la primera es segura y la segunda no lo es.

Compartir la dirección de correo electrónico con un compañero de trabajo es una acción inofensiva que muchas personas realizan normalmente en el trabajo.

Compartir la misma información con una persona que llama y no se identifica podría ocasionar problemas: software malicioso, robo de información personal o incluso una violación de la seguridad en toda la compañía.

Recuerde que la información que puede compartir sin problemas con los compañeros de trabajo puede causar problemas cuando se comparte con extraños, clientes o proveedores. Considere las solicitudes que recibe por teléfono, correo electrónico o en persona y asegúrese de que la persona sea de confianza y de que sea seguro brindarle información.

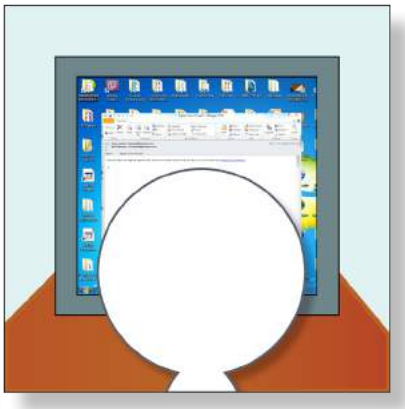
ingeniería social

¿QUIÉNES SON LOS “INGENIEROS SOCIALES”?

Un ingeniero social es una persona que **engaña a otra** para obtener acceso o información. Algunas veces, se les denomina piratas informáticos, estafadores, embaucadores, timadores o impostores y utilizan correos electrónicos, llamadas o visitas en persona para engañarlo y que usted les entregue información que no debería dar. La mayoría de los intentos de robo de información o de llevar a cabo un engaño implican ingeniería social.

Los ingenieros sociales cuentan con que las *personas* sean el eslabón débil en la cadena de seguridad: eso quiere decir que dependen de USTED. Los ingenieros sociales utilizan seres humanos y no técnicas de piratería técnica para que los ayuden a llevar a cabo sus ataques.

En vez de utilizar un software para robar su contraseña, un ingeniero social puede llamarlo haciéndose pasar por un miembro del personal de TI de su organización y simplemente solicitarle la información que necesita.



En vez de tratar de sortear los sistemas de seguridad de su compañía para instalar un software nocivo en su computadora, un ingeniero social puede enviarle un correo electrónico diseñado para engañarlo para que haga clic en el vínculo a un sitio web que hace el trabajo sucio por él. Esto se suele denominar “suplantación de identidad” (phishing).

En vez de piratear el sistema del punto de venta de una tienda para acceder a los números de tarjetas de crédito de los clientes, un ingeniero social puede fingir ser un técnico que necesita acceder al sistema de su tienda.

BLANCOS DE LA INGENIERÍA SOCIAL

Cualquier persona puede ser blanco de la ingeniería social. Es fácil que usted o sus empleados pongan en peligro a su compañía y su información personal por la falta de conciencia.

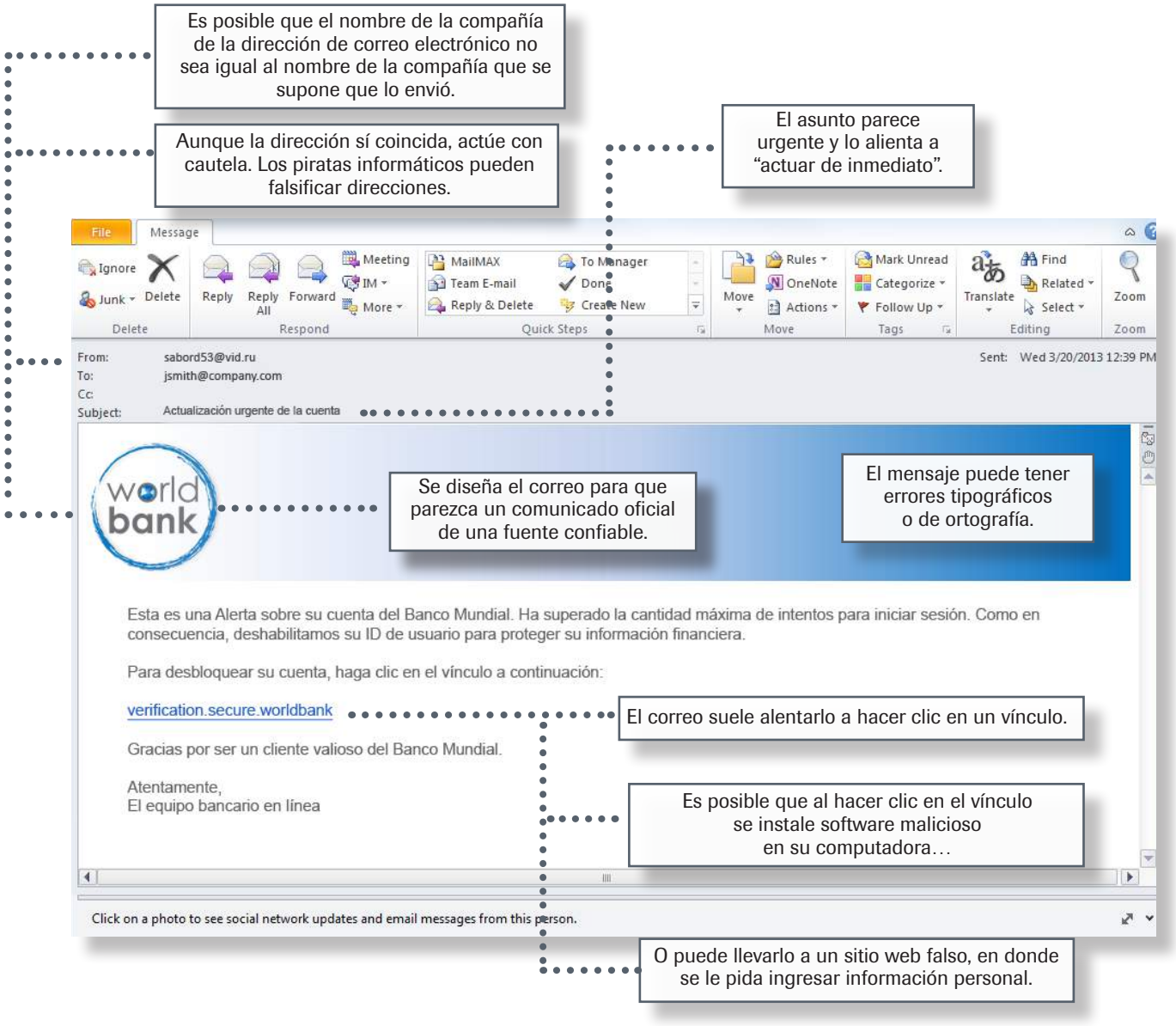
Quizás piense: “Aunque tengo información personal valiosa, como mi número de Seguro Social y los números de tarjetas de crédito, no tengo acceso a ninguna información confidencial en el trabajo. **Dudo que un ingeniero social me elija como blanco”.**

No esté tan seguro. Recuerde que no siempre se puede adivinar cuál es el objetivo del ingeniero social ni cómo podría utilizarse la información. Incluso si la información parece inofensiva y no es confidencial, como en el caso de direcciones de correo electrónico o números telefónicos, es necesario protegerla.

Conclusión: Los ingenieros sociales tienen diversos objetivos y cualquier persona, usted o sus empleados, puede ser el blanco que los ayude a llevar a cabo su estafa. Verifique siempre la identidad de las personas que soliciten acceso a las ubicaciones físicas, los sistemas o la información. Asegúrese de que tengan una necesidad comercial y el permiso para obtener la información o el acceso que solicitan. *Si no está seguro de que deba darle a alguien la información o el acceso a su compañía, no lo haga.*

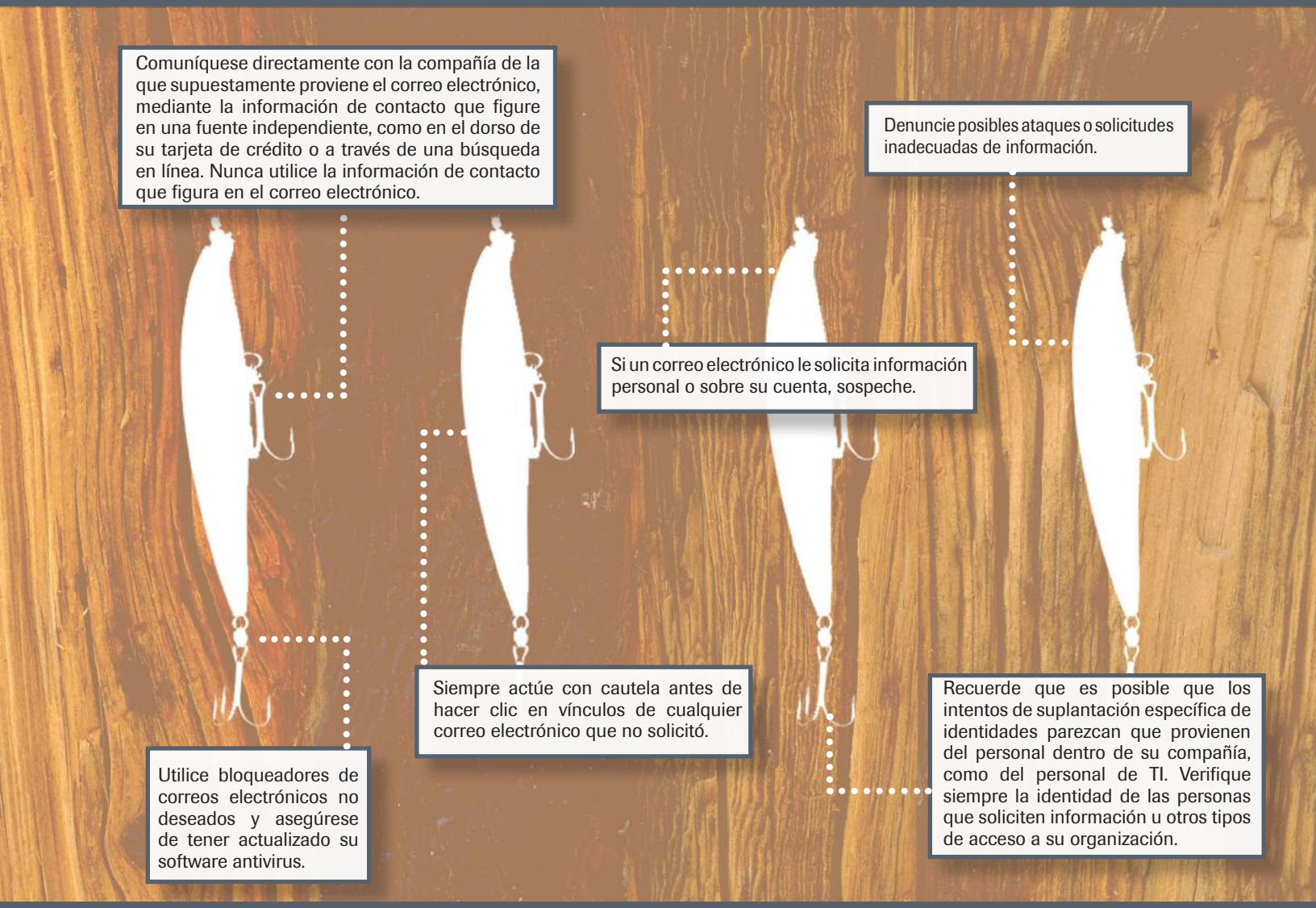
anatomía de un suplantador de identidades

La suplantación de identidad es una treta popular de los correos electrónicos que tiene como fin engañarlo para que brinde información confidencial, mediante el encubrimiento de sus correos electrónicos, con el fin de que parezcan que provienen de fuentes confiables y legítimas. Observe la imagen a continuación para conocer las características más comunes de un correo electrónico de suplantación de identidad.



En algunos intentos de suplantar identidades se envían muchos correos electrónicos con la esperanza de que alguien haga clic en los vínculos que contienen. Otras veces, los correos tienen un objetivo más específico y se envían a ciertas personas en particular, ya que es más probable engañarlas; esto se denomina suplantación específica de identidad (spear phishing). Los correos electrónicos de **suplantación específica de identidad** están bien diseñados y pueden parecer muy reales.

atrapar a un suplantador de identidades



NO SE CONVIERTA EN BLANCO

Los consejos que se muestran a continuación pueden ayudar a disminuir el riesgo de convertirse en blanco de los suplantadores de identidad:

- Nunca utilice su principal dirección de correo electrónico personal ni la de su empresa para inscribirse en sitios web y otros servicios de Internet que no sean esenciales.
- Si no se le solicita su dirección de correo electrónico para inscribirse a un servicio, no la proporcione.
- Cree una dirección de correo electrónico alternativa específicamente para listas de correo y registros en sitios web.

la función de un gerente

CONCIENCIACIÓN SOBRE SEGURIDAD PARA GERENTES

Como gerente o propietario, es su responsabilidad mantener la seguridad de su compañía y de sus clientes. Usted y sus empleados son la defensa más importante que tiene su organización contra los piratas informáticos y otros delincuentes que quieren robar información valiosa. Por eso es tan importante la educación en concienciación sobre seguridad. Las cosas que pueden parecerle inofensivas, como hacer clic en un hipervínculo de un correo electrónico o compartir contraseñas, pueden poner en riesgo información valiosa. Capacitarse en la concienciación sobre seguridad es el primer paso para mantener seguros a su organización y a sus clientes. En las siguientes páginas aprenderá:

- Responsabilidades de concienciación sobre seguridad de los gerentes de ventas minoristas y propietarios.
- Leyes, reglamentos, métodos y las mejores prácticas para mantener segura la información en el entorno de ventas minoristas.
- Cómo proteger la información confidencial y mantener la seguridad.

La responsabilidad de un gerente

Mantener la seguridad de la información es un trabajo en equipo y, como líder del equipo, es su responsabilidad estar al tanto de las leyes y los reglamentos que afectan la información con la que trabaja. Antes analizamos la importancia de conocer las políticas y los procedimientos de su compañía. Además de conocer esas políticas y procedimientos, debe familiarizarse con las leyes y los reglamentos que afectan la información con la que trabaja. A continuación se muestran los reglamentos de seguridad más comunes:

PCIDSS

La Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCIDSS) está compuesta por doce normas diseñadas para proteger los datos de los titulares de tarjetas.

LEYES ESTATALES SOBRE LA PRIVACIDAD

La mayoría de los estados en Estados Unidos tienen leyes sobre la privacidad destinadas a proteger la información personal de los ciudadanos. Estas leyes implican la protección de información confidencial, como números de seguridad social, registros impositivos, registros sobre seguros y antecedentes laborales.

LEY SARBANES-OXLEY (SOX)

La Ley SOX fue aprobada en el año 2001 y exige a las compañías que cotizan en bolsa en Estados Unidos realizar controles internos sobre el proceso de informes financieros, lo que incluye controles de los sistemas de información que almacenan datos financieros.

Conocer las distintas reglas y reglamentos que afectan la seguridad de su compañía es un paso importante para la protección de su información. Además de las reglas y los reglamentos, debe ser consciente de las mejores prácticas que lo ayudarán a evitar que las compañías se conviertan en víctimas.

Las mejores prácticas:

- Las amenazas a la seguridad se encuentran en constante cambio y evolución. Ser consciente de las amenazas más comunes a la seguridad de la información y detectarlas sirve de mucho para mantener segura la información confidencial.
- Asegúrese de mantener a salvo su sistema de punto de venta (POS) y cualquier dato impreso.
- Administre la seguridad de los productos de proveedores que su compañía utiliza. Más adelante en este panfleto, aprenderá más sobre cómo administrar sus proveedores.
- Capacite a sus empleados respecto a la concienciación sobre seguridad y la manera de mantener la seguridad de su empresa.

protección de la información

Saber cómo proteger la información sirve de mucho para evitar una violación a la seguridad de su compañía. Apréndase la información a continuación, compártala con sus empleados y siga utilizando las mejores prácticas.

Amenazas a la seguridad

El primer método para proteger su compañía es conocer las amenazas a la seguridad de la información y tomar las medidas necesarias para evitar convertirse en víctima. Es importante recordar que las amenazas a la seguridad de la información son muy variadas. Los controles de seguridad deficientes, los puntos débiles del software, las identidades falsas y los robos por parte de empleados son comunes; a continuación se ejemplifica cada uno.

Controles de seguridad deficientes
Un restaurante tiene cinco cajas registradoras administradas por un proveedor de servicios externo. El proveedor utiliza un software con conexión remota con el fin de conectarse a las cajas registradoras para solucionar problemas y llevar a cabo el mantenimiento. El software está configurado para que acepte llamadas las 24 horas, los 7 días de la semana, de cualquier número y no solicita una contraseña para conectarse. En este caso, un ladrón de datos puede acceder fácilmente a cada una de las terminales e instalar un software que le enviará los datos de la tarjeta del cliente cada vez que la tarjeta de crédito se pase por la terminal.

Puntos débiles del software
Una compañía ha creado un sitio web de comercio electrónico, pero el software está mal codificado para manejar transacciones de tarjetas de crédito. En este caso, un ladrón de datos puede aprovecharse fácilmente de este punto débil y copiar datos de la tarjeta directamente desde el sitio web.

Identidad falsa
Un "técnico en reparación" recoge una terminal con lector digital de tarjetas para repararla, sin mostrar su identificación. Se retira la terminal de almacenamiento del lugar para su reparación y se coloca temporalmente un lector de tarjetas de reemplazo. En este caso, es posible que el lector de tarjetas temporal que se colocó en la tienda se haya modificado para copiar datos de tarjetas de crédito. Cuando regresa para llevárselo, el técnico podría salir del lugar con todos los datos de titulares de tarjetas que capturó la máquina.

Robo por parte de un empleado
Un empleado lleva la tarjeta de crédito del cliente a un lugar donde este no puede verla, ya sea detrás del mostrador o a otra oficina. En este caso, el empleado podría copiar fácilmente los datos del titular de la tarjeta o incluso pasar la tarjeta por un lector ilegal para capturar la información de la tarjeta del cliente.

Mantenga a salvo los datos impresos

En un entorno de ventas minoristas, es probable que trabaje con datos impresos todos los días. Los informes, recibos y otros tipos de datos impresos con los que trabaja a diario pueden contener información confidencial y siempre deben estar protegidos. Los métodos a continuación ayudarán a mantener sus datos impresos protegidos:

- Almacene la información impresa que contenga datos de titulares de tarjeta en una ubicación segura y bajo llave.
- Verifique los datos impresos almacenados periódicamente para asegurarse de que no hayan sido alterados o robados.
- Asegúrese de que los datos de titulares de tarjetas se almacenen en formato impreso solo cuando sea absolutamente necesario.
- Destruya todo dato impreso que ya no sea necesario con un triturador de papel de corte cruzado o algún otro método seguro.

Administrar los proveedores

Muchas organizaciones utilizan proveedores para instalar y mantener sus sistemas importantes, tales como el sistema de puntos de venta y el firewall. Como resultado, los proveedores obtienen, a menudo, acceso especial a los sistemas de almacenamiento, procesamiento y transmisión de datos confidenciales tales como información de titulares de tarjeta.

Incluso si ha subcontratado responsabilidades comerciales a un proveedor, usted aún es responsable de la seguridad de sus datos. Asegúrese de comprender cuáles requisitos de seguridad cumple su proveedor y verifique que cumpla con la PCIDSS y otras leyes y reglas que le corresponda respetar. Sus proveedores deben cumplir con las normas de la Industria de las Tarjetas de Pago y usted debe poseer un contrato vigente que lo establezca.

Capacitar a los empleados

Como gerente o propietario comercial, se le **exige** que se asegure de capacitar en concienciación sobre seguridad a todos sus empleados que estén en contacto con datos de titulares de tarjeta. Debe capacitar a sus empleados cuando los contrata y brindarles una capacitación de seguimiento una vez al año. Además, debe mantener la concienciación sobre seguridad durante todo el año mediante métodos simples como carteles, reuniones y correos electrónicos trimestrales.

punto de venta (POS)

Proteja su punto de venta

Los sistemas de punto de venta son una parte importante del flujo de datos de titulares de tarjetas y deben protegerse contra amenazas a la seguridad. ¿Qué puede hacer para asegurarse de que sus sistemas de punto de venta se encuentran protegidos?

a) Instalar un firewall: La instalación de un firewall ayuda a evitar que las personas accedan, salgan o vean su sistema sin su permiso o sin que sepa.

b) Instalar software adicional:

- Un control de integridad de archivos (FIM) agrega un nivel de protección adicional contra cambios no autorizados en su sistema.
- Instale un sistema de detección o prevención de intrusos (IDS/IPS); sus sensores ayudan a encontrar y detener el tráfico no deseado de red.

c) Aplicar revisiones de seguridad: Las revisiones de seguridad se crearon para reparar vulnerabilidades de seguridad en el software y sistemas operativos. Asegúrese de que sus revisiones estén actualizadas.

d) Familiarizarse con las medidas de seguridad de su proveedor de POS: Nunca es seguro suponer que su proveedor se está encargando de sus requisitos de seguridad. Asegúrese de que sus proveedores muestren pruebas de sus prácticas de seguridad.

Mantener la seguridad

La concienciación sobre seguridad es un proceso continuo para empleados y gerentes. Manténgase al tanto de las mejores prácticas, los reglamentos y las normas de la industria más actuales. Cree un plan de concienciación sobre seguridad y póngalo en práctica hoy mismo.