LEARNING MADE EASY

AwareGO Special Edition

Cybersecurity

for dummies®
A Wiley Brand

Secure your office and home

Common vulnerabilities and threats

Ten ways to stay cybersecure

Compliments of awarego

Maria Bada, PhD

Ragnar Sigurdsson, CISSP

Cybersecurity

AwareGO Special Edition

**by Maria Bada, PhD,
and Ragnar Sigurdsson, CISSP**

for dummies®
A Wiley Brand

Cybersecurity For Dummies®, AwareGO Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

Registered Office

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

ISBN 978-1-119-72149-9 (pbk); ISBN 978-1-119-72231-1 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Development Editor: Faithe Wempen

Project Editor: Martin V. Minner

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Siddique Shaik

Table of Contents

Introduction

Since the dawn of the Internet, unscrupulous people have been using it to commit crimes. Despite technical advances when it comes to virus protection, unbreachable firewalls, and other guarding methods, cybercriminals are still getting through. How? We simply let them in the front door.

Human error is the most common reason attacks happen. Humans are often unaware of the risks online. They can't see why clicking a link or opening an attachment might be dangerous. Virus protection and firewalls are necessary, but they do little good if we humans keep making mistakes.

Just like firewalls, humans can be programmed to do better. When we educate people about the most common risks and pitfalls of cybersecurity and teach them how to avoid these dangers, they are less likely to make mistakes. They will do better because they know better.

Cybersecurity is not just about buying expensive anti-virus software—it's about the training and programming of *humans* in an attempt to change human behavior. Employees who are well trained regarding cybersecurity will save companies money in the long run, through reduced downtime and direct cost avoidance. More importantly, cybersecurity helps safeguard the company's valuable data and minimizes the risk of regulatory fines.

Small and medium enterprises (SMEs) in particular need to take cybersecurity seriously because not every SME can bounce back after being hacked. Cybercriminals often target SMEs because they are perceived as easy marks due to lack of formal security policies and low security budgets.

About This Book

Cybersecurity for Dummies, AwareGO Special Edition, is a crash course in cybersecurity and how to implement it in a company. This book touches on all the major aspects of cybersecurity and data protection, and helps readers better understand human behavior online.

This book gives you a basic understanding of both the technical aspects of cybersecurity and the human factor. It explains how cybersecurity awareness training is the best way to minimize cyber risks due to human error and why companies should invest in their employees' training. The book identifies the most common methods hackers use to get into systems and what tools administrators can use and offer their employees to minimize the risk of that happening.

Icons Used in This Book

To make it easy to navigate to the most useful information, these icons highlight key text:

REMEMBER

Take careful note of these key takeaway points.

TIP

Follow the target for tips that can save you time and effort.

WARNING

Watch out for these potential pitfalls on the road ahead.

Where to Go from Here

The book is written as a reference guide, so you can read it from cover to cover or jump straight to the topics you are most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome — a better understanding of cybersecurity and better strategies for protecting your organization.

IN THIS CHAPTER

- Describing basic cybersecurity concepts
- Understanding behavior online
- Describing what it means to be safe online

Chapter 1
Introducing Cybersecurity

Smartphones, computers, and the Internet have become fundamental parts of modern life, and with them have come security and privacy threats. From online banking and shopping to email and social media, it is more important than ever for consumers to take steps to protect their identities and data.

This chapter introduces basic concepts related to cybersecurity. It shows you how your online behavior affects your privacy and security, as well as what you can do to be safer.

Defining Cybersecurity

REMEMBER

The prefix *cyber* refers to computers and information technology. *Cybersecurity* is the process and techniques involved in protecting sensitive data, computer systems, networks, and software applications from computer-based attacks.

At its heart, though, cybersecurity isn't only about computers, but about the people who use them — the people who need computers for their work and play, and the bad actors who try to interfere with them doing so. So, cybersecurity is really about

how individuals and organizations reduce the risk of cyber-attacks (that is, computer-based attacks).

Cybersecurity includes a wide range of different measures, concepts, and guidelines, all aimed at protecting computers, servers, mobile devices, and networks connected to the Internet against unauthorized access, data theft, attacks, and manipulation in cyberspace.

The three pillars of cybersecurity are technology, processes, and people. Technological measures can provide the protection needed, but they do not exist in a vacuum. Technologies need processes to govern how they are used. They also need people to use them correctly and to ensure that others are doing so too.

Because cybersecurity has so many facets that depend on one another, it is often referred to as an *ecosystem*. The cybersecurity ecosystem contains a wide range of *countermeasures* (measures designed to counteract attacks). They include technical measures (such as firewalls, cryptography, VPN, or SSL), behavioral measures (such as policies for humans to follow), and legal measures (such as laws that protect people and companies).

Uncovering the CIA Triad


REMEMBER

For a cybersecurity system to be effective, it must offer three things: Confidentiality, Integrity, and Availability. Together these are known as the *CIA Triad.* This section looks at each of these in more detail.

Confidentiality

Confidentiality defines the rules that limit information access. For example, an organization's security system allows or denies employees access to information according to the employee's job function and the data's category.


TIP

There are many ways to ensure confidentiality, such as two-factor authentication, data encryption, data classification, biometric verification, and security tokens. Upcoming chapters look at these in greater detail.

Integrity

Integrity assures that data is consistent, accurate, and trustworthy wherever it is: in use, in storage, or in transit. No matter where the data is, or who is using it, cybersecurity measures such as file permissions and user access control ensure that it is not changed, altered, deleted, or illegally accessed. Additional tools and technologies detect any change or breach in the data.


TIP

Regular backups provide some insurance against data loss caused by cyberattacks, accidents, and natural disasters. *Cloud-based* systems provide secure applications and storage online that people can access from anywhere in the world using an Internet connection.

Availability

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format. If authorized users cannot get to the data they need quickly, when they need it, that's a big problem.


REMEMBER

Confidentiality and integrity both tend to increase when security is tightened, but the same cannot always be said for availability. Often when a system is heavily secured to ensure confidentiality and integrity, availability suffers. To take things to their most extreme, a server that doesn't allow any users or network connections would be very secure — but what good would it be to anyone? Not much good. Sometimes trade-offs between availability and security are necessary.

Understanding Online Social Behavior

Online social behavior refers to people's online interactions with one another and with groups or organizations. It includes positive (or at least neutral) behaviors like social networking and self-representation, as well as anti-social behaviors such as cyberbullying. A person's online social behavior choices do not just create their online presence; they can also make the person less or more vulnerable to cyberattacks.

Many people say and do things in cyberspace that they wouldn't ordinarily say and do in the face-to-face world. They feel less restrained and express themselves more openly. This phenomenon is called the *online disinhibition effect*. Disinhibition means just what you might guess — a lack of inhibition.

Disinhibition happens frequently online because people can be anonymous and invisible and can create multiple different identities. They also may be interacting with people asynchronously (that is, not at the same time) because they are in different time zones. The online disinhibition effect tends to bring out people's true natures, for better or for worse.

Disinhibition can lead people to disclose more about themselves online than they would in real life, because it seems "safe" to do so. It might feel rewarding and affirming to join online communities and talk openly about their lives. However, this kind of open sharing also can make them a target for cybercriminals looking for exploitable information.

Trust plays a big role in how people behave online. Systems trust users based on their authentication credentials. Users trust websites based on their legitimacy. People might trust the links in each other's emails based on friendship and familiar email addresses. Trust and influence are entwined. Part of staying safe online is understanding who and what we can trust — and who and what we can't.

We allow ourselves to be influenced by those we trust, but we can also elicit trust by wielding influence skillfully. And that's a major area that cybercriminals exploit.

Staying Safe Online

Internet safety or online safety is all about maximizing the user's personal safety and privacy. This can include avoiding security risks, guarding private information and property, and being savvy about identifying scams and deceptions. Here are some simple security measures that can help protect people, organizations, and their data.

Making sure your Internet connection is secure

At home and at work, most people use a known, password-protected router that encrypts their data. *Encryption* is the process of encoding data so that it is unreadable unless you have the corresponding key. Encryption makes data more difficult to steal, so it prevents some cyberattacks.

But when people are on the road, they are often tempted to use free public Wi-Fi provided by a router of unknown ownership. Anyone — including a would-be cybercriminal — can set up a router in a public place and label it *Free Wi-Fi.* Unsuspecting users who join the network to get Internet access put their systems at risk for security and privacy violations.


TIP

One way to safely use an unsecure Internet connection is by using virtual private network (VPN) software. A VPN is an application that creates a secure "tunnel" through an unsecure network, usually the Internet. This tunnel enables users to connect securely and privately to a remote network.

Being careful what you download

Many of today's online threats are based on getting people to click the wrong link. After clicking a bad link, people are tricked into revealing personal or sensitive information for fraudulent purposes. Internet users should be wary of offers that sound too good to be true or when sites or programs ask for too much information.

Choosing strong passwords

Creating complex, unique passwords can successfully prevent an attack. Reusing passwords for multiple accounts can make it easy for hackers to gain access to multiple accounts. All they need to do is steal a password from one site, and they suddenly have access to accounts on all the other sites where that same password was used.


TIP

A password manager can help store and create strong, unique passwords for multiple online accounts.

Making online purchases from secure sites

When shopping online or visiting websites for online banking or other sensitive transactions, always make sure that the site's address starts with *https*, instead of just *http*, and has a padlock icon in the URL field. This indicates that the website is secure and uses encryption to scramble data so it cannot be intercepted by others. Avoid websites that have misspellings or bad grammar in their addresses.

WARNING

Cybercriminals often set up fake versions of well-known sites with URLs very similar to the real ones. Victims are directed to the fake site if they mistype the site they want.

Being careful when meeting someone online

Not everyone who is friendly online is your friend. Some scam artists try to ingratiate themselves with lonely people online, with a goal of getting them to send them money — or to disclose personal details they can use to steal something from them. Others may try to get you to meet them in person so they can then rob or even kidnap you. Children are especially vulnerable to online predators.

Keeping your operating system updated

Every operating system (OS) is potentially vulnerable to security attacks, and cybercriminals are constantly probing the popular OSes to find weaknesses they can exploit. As soon as these vulnerabilities are discovered, the company releases a patch or update to fix them. Not everyone updates their OS immediately when a fix is released, though, and criminals use that oversight to their advantage. To keep your computers as secure as possible, you should immediately install OS updates when they become available.

Protecting your wireless network

Many households have wireless routers that they use to share the Internet connection with multiple devices. By default, home wireless routers do not have security set up on them. Anyone nearby can use the shared Internet connection — and potentially connect to other devices using it.

To prevent random people driving by your house from getting onto your network, configure your wireless router so that it requires a security key (essentially a password) to connect to it.


TIP

For extra Wi-Fi security, you can also configure the wireless router to hide its service set ID (SSID) — its name — so that only those who know its SSID can connect to it.

Using a firewall

A *firewall* is an electronic barrier that prevents unauthorized activity through the computer's ports. Firewall software is often included with a suite of security utilities, and many network hardware devices (like wireless routers) can also serve as firewalls. Using the firewall features of your home router ensures that all the devices connected to a network are secured, including Internet of Things (IoT) devices like smart thermostats and webcams. This precaution is important because many IoT devices are not equipped with security measures, giving hackers a vulnerable point of entry to the entire network.

Being a selective sharer

Be cautious about what you share online, particularly details pertaining to your identity. Any information you provide can be used to guess your passwords and logins, impersonate you, and even target your home or family for crimes.

Securing your mobile devices

Mobile devices like tablets and smartphones can be as vulnerable to online threats as laptops. In fact, mobile devices face additional risks because of the ease with which they can install new applications. If you receive a message with a link to a "great new app" that isn't available in the officially sanctioned app store, it may be a scam designed to trick you into installing malware that steals your private information or holds your data for ransom. Be careful where you tap, don't respond to messages from strangers, and download apps only from official app stores after reading other users' reviews first.


TIP

It is just as important to use security software on mobile devices as it is on a computer.

IN THIS CHAPTER

- Learning why humans are the weakest link
- Exploring SME technology vulnerabilities
- Decreasing attack vulnerability
- Dealing with the aftermath of a breach

Chapter 2
Understanding SME Vulnerabilities and Threats

Small- and medium-sized enterprises (SMEs) are often the targets of cybercrime because they tend to have weaker defenses. Not only can many not afford top-tier cybersecurity hardware and software and its maintenance, but they also often can't afford to hire the most knowledgeable and experienced cybersecurity staff. As a result, bad actors accurately see SMEs as easier and more appealing targets.

SMEs in regulated industries typically have at least the minimum security in place to meet regulations, but compliance alone does not guarantee protection from attack, nor resilience in recovering from one.

People are the primary target of attackers and the last line of defense for organizations, making a focus on people, as well as more traditional layers of security and training, critical to a holistic approach to defense. It is especially important for SMEs to develop a strong security culture, something that can also help address many of the behavioral issues that underpin security

failures. Network, website, and mobile technologies are all especially vulnerable to technological attacks, and vigilant SMEs put multi-layer protections in place to make it as difficult as possible for threat actors to attack their technology.

This chapter explains how SMEs are especially vulnerable in these two areas and offers some suggestions for minimizing the risks. We also touch on how to deal with the aftermath of a breach.

People: The Weakest Link

The modern threat landscape is increasingly "people-centric." With many attacks focusing on people and identities rather than infrastructure these days, it is important to identify which users in an organization represent the greatest sources of risk and do everything possible to prevent their accounts from being compromised.

The majority of attacks exploit "the human factor," the instincts of curiosity and trust that lead well-intentioned people to click, download, install, open, and send money or data. Regardless of the target or the motivation of an attack, people are the most effective vectors to infiltrate organizations and facilitate fraud and theft.

Cybercriminals typically rely on human interaction rather than automated exploits to install malware, initiate fraudulent transactions, steal data, and engage in other malicious activities. Even automated exploits are frequently deployed in ways that still require a human to set them off, such as a click on a bad hyperlink or opening a malware-infected attachment.

Identifying VAPs

Every organization has a subset of users who are more easily attacked than others. They are commonly referred to as *Very Attacked People (VAP)*. VAP accounts include accounts that are easily discovered or targets of opportunity like shared public accounts. Threat actors find VAP-associated identities online through corporate websites, social media, and publications. You might expect that top executives would be prime targets, but that isn't always the case. The accounts that have the most ability to compromise systems are often mid-level workers in finance, marketing, or education positions.

VAP accounts carry the highest risk of attack and suffer the greatest attack severities because of the potential for the attacker to carry out their aim. For example, a personnel officer's account may have access to sensitive personnel data that can be used to determine the targets of future attacks, and a finance officer's account may be able to move funds in a wire transfer scheme.

To identify the organization's VAPs and potential harms, ask questions such as:

- Why would someone want to attack our business? What would they hope to get out of it?
- Which accounts have the privileges a threat actor would target to accomplish their aim?
- With which accounts could an attacker do the most damage to us?

VAP accounts should be fortified with extra security measures, such as multi-factor authentication, and the users holding those accounts should receive additional security training.

Educating Your Employees About Security

All employees must be aware of their role in minimizing cyber threats. Providing simple and practical advice to employees on the organization's mission and resources is vital, as is encouraging good security behavior.

REMEMBER

Cybercriminal strategies are people-centric, and this is exactly the approach SMEs need to follow.

TIP

Here are some recommended measures:

- **Adopt a people-centered security posture.** Consider the individual risk each user represents. Think about how they might be targeted, what data they have access to, and how technically savvy they are.
- **Train employees to spot and report attack attempts.** Providing training and testing users with simulated attacks can help stop many attacks and can help identify vulnerable users.

- **Assume that employees will eventually do something to compromise systems.** Attackers will always find new ways to exploit human nature. Implement solutions that spot and block inbound email threats, such as isolating suspicious and unverified URLs in emails.
- **Build a robust email fraud defense.** It can be hard to detect email fraud with conventional security tools. To strengthen your defense, invest in solutions that manage email based on custom quarantine and blocking policies.

Exploring Technology Vulnerabilities

A *vulnerability* is a weak spot in an organization's security that might be exploited by a security threat. The most common technology vulnerabilities that SMEs face are network, website, and malware related:

- **Network vulnerabilities:** SME networks are often vulnerable because of factors such as aging hardware, old software versions, and failure to carry out regular system updates. An exploited network can result in loss of data, hours or days of downtime, and staff time needed to rebuild the network systems.
- **Website vulnerabilities:** SME websites may not be as robust and bullet-proof as sites of larger companies. A successful web attack can allow a threat actor to get control over an organization's website and steal sensitive data, causing significant reputational damage and financial losses. Web applications in particular are susceptible to many types of attack.
- **Mobile malware:** Small organizations often adopt a "bring your own device" (BYOD) culture in which employees are allowed to use personal mobile devices on the company network, often without receiving any training on the threats associated with mobile devices or on practices such as encrypting mobile phone data. As a result, private mobile devices are often the source of malware coming into the company's network.

Decreasing Attack Vulnerability

Not all organizations have the necessary resources to fully address the business-critical issue of cybersecurity, but nearly every company can improve its security by rigorously practicing some simple technological hygiene. The following sections explain five key areas that any SME can focus on: patches, secure configuration, firewalls, access control, and malware protection.

Patches


REMEMBER

Any software is prone to technical vulnerabilities. Once discovered and shared publicly, these can rapidly be exploited by cybercriminals.

Patch management refers to keeping software on computers and network devices up to date and capable of resisting low-level cyberattacks. Patch management is essential for effective cybersecurity. In order to avoid a breach due to not updating devices, companies need to ensure that all their software is:

- **Licensed and supported.** Unlicensed or expired copies of the software may not be updatable.
- **Removed from devices when no longer supported.** Software that isn't being actively patched by its manufacturer leaves the system at risk of an attack if a vulnerability is found.
- **Patched within 14 days of an update being released, especially if a vulnerability is critical.**

Secure configuration

Secure configuration refers to security measures implemented when building, installing, and setting up computers and network devices to reduce unnecessary vulnerabilities. Security misconfigurations are one of the most common gaps that cybercriminals look to exploit.

For example, a network router has many security settings that can be configured in many different ways — and some of those ways make it much easier to attack than others. Accepting the default settings without reviewing them can create serious security issues

and can allow cybercriminals to gain easy, unauthorized access to your network and data.


REMEMBER

It is not difficult for online offenders to identify the default password set by the manufacturer of a certain brand or model of hardware. Many manufacturers use the same default settings for all devices and models.

Examples of devices or systems that need to be configured are routers and other network hardware, operating systems (client, server, and mobile), and web servers.


TIP

Here are some specific tips:

- **Switches and routers:** Change the default administrator password immediately upon deployment.
- **Wireless routers and access points:** Enable security encryption, use a robust security key for user connections, and prevent SSID broadcast.
- **Autorun:** Disable any auto-run features that automatically run executables when discs or drives are connected.
- **Applications:** Remove or disable unnecessary applications.
- **Web servers:** Configure the web server software to ensure robust security, and limit administrator access to those who need it.
- **Computers:** Configure user accounts with security levels permissive enough to allow users to do their work but no more than that.
- **Network devices:** Make sure all network devices enable any built-in security available. Keep the device firmware updated, as firmware patches sometimes introduce more robust security measures.


WARNING

Many businesses use cloud computing services, especially for data storage and computing power. The complexities of a cloud environment (particularly a hybrid cloud environment) make configuration more challenging than would be the case in a single-location, homogenous network. A cloud provider must enable service for clients in various locations, using all different kinds of hardware and software. It is important, particularly for SMEs, to understand how their cloud resources are set up and accessed.

Firewalls

A *firewall* helps keep attackers or external threats from gaining access to a system through the Internet. It monitors all network traffic and can identify and block unwanted traffic that might be harmful to computers, systems, and networks.

A firewall creates a barrier between the Internet and a computer or network. A firewall can help protect against:

- Breaches by criminal hackers
- Malware such as worms that spread from computer to computer over the Internet
- Some outgoing traffic generated by malware

TIP

To secure their firewalls (or equivalent network devices), organizations should:

- Change default administrative passwords on all devices, or better yet, disable remote administrative access entirely.
- Block unauthenticated inbound connections by default.
- Remove or disable permissive firewall exceptions as soon as they are no longer needed.
- Use software-based firewalls on host devices that are used on untrusted networks, like public Wi-Fi hotspots.

Access control

If your organization has employees who connect to the Internet, you need some type of access control. *Access control* authenticates user identities and authorizes them to access information. It consists of two elements:

- **Authentication:** Verifying the identity of a user.
- **Authorization:** Determining whether a user should be given access to certain data.

User accounts should be assigned only to people who need them, and that's especially true for accounts that have higher-than-average access privileges, such as administrative accounts. All

accounts should be managed effectively and should provide only as much access as the user requires to get their work done — and no more.

TIP

Organizations must define an appropriate access control model based on the type and sensitivity of their data. A model that makes sense for a company handling highly sensitive health or financial data is very different from one that handles mostly data of low value to attackers, such as product specification databases or maintenance schedules.

Here are some tips for effective access control:

- Authenticate users using unique credentials before granting access to applications or devices.
- Remove or disable user accounts that are no longer required.
- Assign the fewest privileges to each account while still permitting the account holders to do their jobs (the *principle of least privilege).*
- Implement two-factor authentication when possible.
- Use administrative accounts only to perform administrative activities; require system administrators to use standard accounts for everyday routine activities.

Malware protection

Malware protection is important because malware attacks are one of the main threats organizations face daily. Malicious programs can be delivered physically to a system through a USB drive or other means, or via the Internet through downloads.

Guarding against a broad range of malware and having well-defined procedures for virus removal protects computers and important data from attacks. These measures likewise safeguard user and company privacy.

REMEMBER

Malicious websites and phishing scam emails that contain malicious links or attachments are two common delivery methods.

Organizations need to:

- Equip all computers and mobile devices with robust anti-malware software and keep it up to date.
- Configure anti-malware software to scan files automatically when accessed.
- Use an anti-malware solution that scans email messages and their attachments.
- Ensure the anti-malware software scans web pages automatically as they are accessed through a web browser and blocks connections to sites found to contain malware or other threats.

Dealing with the Aftermath of a Breach

An important part of any cybersecurity strategy is how to deal with a security breach after it has happened. Cybercrime often has serious economic consequences for the victims, whether individuals or companies. SMEs are especially hard hit, not having the deep financial reserves that may be needed to recover.

In the short term, a checklist of steps to take to recover account security should be followed. This can include tasks like changing passwords, getting new account numbers, freezing credit cards, changing phone numbers, and restoring data from backups.

In the longer term, organizations should provide education on what happened and how it can be prevented from happening again. A thorough inspection of the organization's computer systems and processes must take place to find out where they are lacking.

REMEMBER

Cyberattacks can not only cost individuals, companies, and even governments financially, but can also cause their reputation to suffer.

Accurate or not, there is a perception that a company suffering a cyberattack somehow brought it on itself by not hardening its security systems and training its users adequately. Such a reputation hit to a company can be devastating. The perception of a company being "soft on security" can cause long-standing customers to take their business elsewhere and can turn away potential new customers.


TIP

To mitigate the effects of a potential cyberattack on a business's reputation, companies must be proactive. Their disaster recovery plans should include a response plan specifically for cybersecurity breaches, with sections that explain in detail how they will:

- Immediately stop the breach and assess its impact
- Inform the appropriate personnel
- Take steps to prevent the breach from happening again
- Quickly craft a public announcement that minimizes reputational damage
- Manage an ongoing public relations campaign to restore public confidence in the company

IN THIS CHAPTER

- Understanding social engineering
- Comparing social engineering approaches
- Avoiding phishing attacks

Chapter 3
Defending Against Social Engineering

Cyberattacks are becoming more common, and cybercriminals more effective in exploiting the human factor (in other words, *people*). As Chapter 2 explains, people are often the weakest link in the security chain and the easiest target for criminal activity.

One of the main techniques used for a data breach is social engineering. Social engineering has evolved from simple spam emails tricking users into clicking bad links into advanced technologies such as data analytics, cognitive science, and automation.

This chapter explains the most common social engineering attack types and suggests some ways to defend yourself and the users you support.

Understanding Social Engineering

Social engineering is the practice of convincing people to compromise information systems. Instead of targeting equipment or software, social engineers target humans who have access to information and manipulate them into divulging confidential information using

deception, influence, or persuasion. Technology-based protection methods are usually ineffective against this kind of attack.

REMEMBER

Social engineering attacks can include physical, social, and technical aspects, which are used in different stages of the actual attack. What they all have in common is involvement with a human victim or enabler. Some of the ways social engineers attack include email, instant messaging, phone, social networking, cloud services, and websites.

The originator of an attack can be either a human or software. Human attacks can be more psychologically nuanced, but the number of attacks they can launch is limited because they're slower and less efficient than software. Software-based social engineering attacks are less common, but they do happen.

Social engineering attackers use many tools and techniques. What these social engineering methods have in common is that they all attempt to build rapport with individuals by creating believable situations, establishing credibility, and creating a sense of urgency. This chapter explains several categories of these techniques.

WARNING

The very human traits and behaviors that make employees valuable to a company can also make them vulnerable to attacks. The main psychological factors being exploited by criminals are:

- **Trust:** People want to trust others. Exploiting that impulse is the basis of social engineering.
- **Ignorance:** People don't recognize social engineering attacks for what they are. Lack of knowledge about social engineering attacks makes people and organizations vulnerable.
- **Fear:** People are afraid of loss, and fraudsters exploit people's fears. For example, they might send a message or make a call warning about possible loss of employment or money.
- **Greed:** People want money. Social engineers promise rewards in exchange for divulging information.
- **Moral duty:** People want to be helpful. They often feel obliged to help social engineers when asked for help.

- **Curiosity:** People want to know things. A fraudster might send an email with a subject line such as "Unusual sign-in activity" or "Unusual ATM withdrawal," making the recipient want to know more.
- **Urgency:** People are sympathetic to someone who appears to have an urgent need. A fraudster might call or email in the guise of a high-ranking chief executive officer or chief experience officer who requires an urgent transfer of funds or company data.
- **Recognition:** People want to be noticed and appreciated. A fraudster might send an email with a subject line promising money or fame such as "You have won the Excellent Performer award."
- **Panic:** People don't think clearly when they're pressured to act quickly. A fraudster might call or send a message that insists the recipient take immediate action.
- **Anger:** People are uncomfortable when someone else is angry at them. A fraudster might pretend to be someone with authority who is angry about a situation that the recipient can remedy by breaking the rules.

Comparing Social Engineering Approaches

Social engineering techniques follow different vectors (that is, approaches). Here are some of the most common ones:

- In-person visits where the attacker impersonates someone in authority or someone with an urgent need
- False documents intended to deceive
- Telephone calls where the attacker impersonates someone in authority or someone with an urgent need
- Email messages that are either false in content or false in origin
- Instant messages or SMS text messages with false threats, information, or promises

In each of these approaches, deception is the key, with impersonation and disguise implemented either by speech, documents, or physical disguise (for example, wearing a uniform).

WARNING

Social engineering attacks involving email or messaging require little effort because they can be automated, and they can easily reach thousands of potential victims.

Phishing

REMEMBER

Phishing is the process of contacting individuals, usually by email or telephone, posing as a representative of a legitimate institution. The goal is to lure the individual into providing sensitive information such as banking information, credit card details, and passwords.

Some classic examples of phishing email techniques are subject likes like these:

- Luring emails that arouse greed or curiosity like *You have won a lottery prize* or *Attached is your travel confirmation.*
- Urgent emails with frightening warnings like *Your account will be terminated unless we hear from you* or *IRS audit warning*.
- Links to other websites that look legitimate, such as a message that directs you to a fake version of your bank's website or the details for a shipment.
- Spam emails that advertise non-existent or substandard products and services, asking for your credit card information to pay for them.

There are several sub-types of phishing, each one targeting a specific type of person or doing so in a specific way. Learn about these in the following sections.

Spear-Phishing

General phishing schemes cast a wide net, sending out thousands of email messages indiscriminately and then exploiting whoever is naïve enough to respond to them. *Spear-phishing* attacks, in contrast, are phishing attacks that are targeted at specific individuals or companies.

Spear-phishing targets are usually selected based on demographic, financial, or employment information. For example, a message might be targeted to customers of a bank or Internet service provider, or employees of a certain company. Because it is targeted that way, spear-phishing requires the attacker to first gather enough information on the intended victims to learn that they fall into the target group.

Having some information about the potential victim enables the threat actor to enhance the appearance of legitimacy, making the con more effective. Because the website or message looks legitimate (for example, containing the right logos and names), the target person is less likely to scrutinize it closely.

Vishing

Phishing attacks that occur over the phone are known as *vishing*. (Vishing is a combination of *voice* and *phishing*.) They attempt to socially engineer the intended victim into providing personal, financial, or other confidential information for the purpose of financial reward.

WARNING

You might think you can detect a known person's voice over the phone, but new technologies are making vishing fraud much easier to pull off. Nowadays deep fake algorithms and voice imitation applications such as Lyrebird make it easier for voice imitation, enhancing the success of vishing attacks.

Smishing

The term *smishing* refers to phishing attacks via text messages (especially SMS, but including other forms such as WhatsApp as well). Smishing derives its name from the text messaging technology SMS (Short Message Service). SMiShing . . . get it?

These are two common smishing scams:

- The victim receives a text message that seems to originate from a known and trusted source, such as your bank or your system administrator.
- The victim receives an urgent text message about their identity being stolen or account number being frozen. It then directs them to a website or a phone number for verification.

Whaling

Whaling refers to spear phishing attacks that target senior executives and other high-profile targets. Many corporate websites and professional networking systems like LinkedIn provide lots of biographical and professional information about a company's executives, so they are fairly easy to target.

Two common whaling techniques are:

- **C-Level email impersonation:** The term *C-level* refers to positions in an organization that start with the letter *C,* such as chief executive officer (CEO) or chief financial officer (CFO). Scammers pose as CEOs or CFOs as they reach out to the target individuals to give their communication a feeling of legitimacy and urgency.
- **Business email compromise attacks:** Hackers infiltrate legitimate business email accounts and send out emails that seem to be from the executives, authorizing information release and fund transfers.

Avoiding Phishing Attacks

No matter how small and low-profile a business is, its employees will inevitably receive phishing messages.

TIP

Here are some tips to help identify the most common phishing attacks:

- Be wary of short, generic messages.
- Double check a link before clicking or downloading.
- Never send sensitive, personal, or proprietary information via email, regardless of who is asking for it.
- Scrutinize received emails that were sent to large groups.
- Make sure the organization has a procedure for all requests involving sensitive information or payments and make sure people follow the procedure.

IN THIS CHAPTER

- Recognizing the risks of working remotely
- Addressing remote security challenges

Chapter 4
Working Remotely

Workers and employers are increasingly finding it advantageous for employees to "work from home" or from some other remote location. Remote workers can employ various means of staying in touch with the company, such as by telephone, text messaging, and video conferencing, as well as using virtual private network (VPN) connections to access the company servers. Workers get convenience and freedom, and their employers get lower turnover and lower office expenses. It's a win-win for many positions.

When employees and their computing devices aren't physically in the building, though, it can be more difficult to control security and privacy. Having many workers routinely logging into the company networks remotely can make it harder for IT staff to spot unauthorized logins and credential theft, for example. Security is also an issue when employees use their own laptops and phones rather than company-issued ones.

This chapter looks at some of the risks that employers and employees face with remote work and explains some of the ways to decrease those risks to an acceptable level.

Recognizing the Risks of Working Remotely

Expedience and security are often at odds with one another, and remote work situations are an excellent example. Working from home is certainly expedient and convenient, but it introduces some IT security challenges. Here are some of the most significant ones.

Unsecure networks

When workers access company assets via the Internet, they can potentially do so from anywhere — their own homes, a coffee shop down the street, an Internet café halfway around the world — anywhere at all. That's great! But it can also pose a security risk.

Using a public network increases the risk of a potential data breach or other security leaks. Whenever a person takes advantage of a free public Internet connection, like at a restaurant, airport, or public building, they assume that the company or person generously offering that free connection is not a malicious actor. That isn't always a safe assumption. Whoever controls the router can set up software to capture all the network traffic and sift through it looking for passwords, credit card numbers, and other personal data. In some cases they can also take advantage of naïve users' lax security settings to snoop in their file systems.

Personal and shared devices

REMEMBER

You can caution employees against using company-issued computing devices for personal matters, but that's hard to enforce. System administrators can set up some operating system permissions to prevent certain risky activities, like installing new software, but it isn't a perfect system.

Keeping unauthorized users off a work PC can also be a challenge. If a computer is in someone's home, how do you prevent family members and housemates from using it and introducing extra security risks?

So if you don't want employees playing fast and loose with company-owned equipment security, what if you let them use

their personal devices for work? That is even *more* of a risk, because you can't be confident that the devices have adequate security measures in place. When employees use their personal devices, they feel justified in installing whatever software they want — possibly including shady or unreliable software that leaves the computer open to malware attacks. When malware and company data are together on the same computer, the data is no longer safe.

REMEMBER

The bottom line: Employees should have separate devices for work and personal use, and should be strongly advised not to mix them.

Insecure mobile devices

Many people have some work-related apps and data stored on personal mobile devices, like a company-created app for accessing the company's databases or email servers. And whenever there's company data on a private device that IT can't control, there's risk from hacking, malware, and phishing.

Virtual meetings

Many remote employees use online collaboration tools such as Zoom and Slack to stay connected to co-workers and clients. Although such tools are convenient, they are also hackable apps. When they're on private devices, they're even more at risk because users don't always install security updates and patches immediately.

Addressing Remote Security Challenges

You can't make every work-from-home situation completely secure, but you can take steps in that direction. Here are some of our best suggestions.

Have a risk management policy

Companies take strategic risks by allowing employees to work remotely. Working remotely creates many security vulnerabilities, so the expected benefit must be compelling for a company to voluntarily take such a risk. A *risk management policy* explains how the company and its employees recognize and control the potential risks that are inherent in certain activities (like working from home).

Whereas the remote work policy is a set directive for the end users who will be working remotely, a risk management policy is more of a strategy document that outlines the company's philosophy and approach.

Have a remote security policy

Any company that permits staff to work from locations other than the office must have a well-defined set of employee policies for doing so. A remote work policy can help reduce the inherent risks of working remotely by spelling out exactly what employees can and can't do, and in some cases how they should do what's permitted.

The policy should include the following procedures:

- A process for approving employees to work remotely
- Well-defined employee responsibilities
- Instructions for securing remote workspaces
- Steps for workstation or device security hardening
- Instructions for enabling data encryption for both information storage and information transit
- Instructions for setting up and using a VPN connection, and a mandate to use it
- Instructions for reporting security incidents

Offer the right tools

For employees to follow the policies you set to keep their devices and data safe, you must provide them with the right tools and technologies. Here are the most important ones for them to have:

- **Virtual private networking (VPN)** is a way of creating a secure tunnel through an unsecure network (the Internet).
- **Encryption** makes it much more difficult for thieves and hackers to pull data off a device should it be lost or stolen.
- **Password managers** help users store and recall their passwords and generate secure ones. A password manager makes using strong, difficult-to-guess passwords less inconvenient for employees, so they are more likely to do that.

» **Firewall software** can prevent inbound or outbound requests that could be malicious. Firewall software should be enabled on all endpoint devices, including laptops, tablets, and smartphones.

Keep devices patched and up-to-date

IT teams need to ensure that staff understand the importance of keeping software (and the devices themselves) up to date, and that they know how to do this. Most operating systems are self-updating these days, but not all applications are, and sometimes firmware updates may be required as well for optimal security.

Encourage good basic digital hygiene

Employees should be trained and encouraged to use common-sense security best practices. Not sharing a work computer with friends and family, using a single sign-on service or password manager, and enabling two-factor authentication are some ways to make data breaches far less likely.

Give clear security guidance

Although each business will have its own protocols, one important part of this process is remaining clear and consistent in making those protocols known to all employees, remote or not. For example, a company must inform employees that they are not allowed to connect to public networks from work devices.

Use cloud software solutions for file management

Companies should encourage employees to avoid removable storage devices such as USB drives to store sensitive files. They can easily be stolen, or their data transferred to other devices. Instead, advise employees to use secure cloud-based storage solutions such as Google Drive or Dropbox.

Take extra precautions during virtual meetings

Remote workers often rely on video conferencing to collaborate at a distance. The ideal video conferencing solution provides these capabilities:

- **Control meeting entry.** Meeting organizers should be able to control who can attend the meeting to avoid uninvited or unwanted attendees.
- **Password-protect meetings.** Being able to password-protect meetings allows the organizer to control the attendee list.
- **Manage secure access to content**. To prevent unauthorized individuals from downloading content during a video conference call, the meeting platform should enable organizers to manage content sharing settings.

Training and best practices

Having a security policy and supporting it with the right tools is important but educating and training employees on best practices will help them understand *why* they need to follow the policy and use the tools. A short security training course can encourage workers to remain alert and avoid risky behaviors like clicking unknown links and accidentally downloading infected documents.

Employees working from home must receive basic security advice: to beware of phishing emails, to avoid use of public Wi-Fi, to ensure home Wi-Fi routers are sufficiently secured, and to verify the security of the devices they use to get work done.

REMEMBER

Along with basic security guidance, employees need to know who to contact if they detect a security threat.

IN THIS CHAPTER

- Implementing a successful security awareness strategy
- Measuring information campaign effectiveness
- Developing a cybersecurity culture
- Promoting information security awareness to the C-suite

Chapter 5
Developing an Information Security Awareness Strategy

Organizations of all sizes must have a cybersecurity strategy, but it is especially critical for small- and medium-sized businesses. That's because these businesses don't typically have the financial resources needed to recover from serious security breaches. An effective cybersecurity strategy can make the difference between a thriving business and a bankrupt one.

An important part of a cybersecurity strategy is an *information security awareness strategy*, which is a plan for making sure employees understand how their actions affect the company's overall cybersecurity. In this chapter, we explain how to develop and run an information security awareness strategy, measure its effectiveness, and create a strong cybersecurity culture.

Developing an Information Security Strategy

Developing an effective information security awareness strategy is a multi-step process that begins with identifying the people who need to be involved. For example, for a small or medium enterprise, the business owners and employees would certainly have input in crafting the policy, and perhaps third-party suppliers and contractors would have helpful input as well.

After the development team has been assembled, the next step is to analyze the organization's current situation, identifying what people already know and what they still need to learn regarding cybersecurity. The team can address any risks they identify by developing plans specific to those risks. For example, if there has been a recent breach — or threat of one — training can be focused in that area.

The development team then defines the goals to be achieved and comes up with strategies to achieve them. For example, perhaps they conclude that the organization needs a shift in employee attitude and behavior, and they propose ways to make that happen, like conducting in-person or online training, creating a special section of the company's internal website, and sending out periodic security reminders via email. The exact strategies depend on the company's people, technologies, and processes. (We provide ideas later in this chapter.)

Another important consideration is the resources required (financial or expertise related) to implement the plan. Do you already have people on staff who can conduct the needed training? Do you have people with the writing skills to craft the written policies? How much will it cost to do all that?

Once the overall plan has been defined, the team (or designated others) can work on the specifics of bringing it to life, which the next section covers.

Implementing the Strategy

Implementing your information security awareness strategy is a matter of "getting the word out" to employees and other interested parties (such as contractors and vendors) about the company's cybersecurity goals, initiatives, and policies.

TIP

As you implement your strategy, it's important not to bog people down with too much technical detail. Keep it simple. Tell them what you want them to do, and why it's important. Make sure they understand how to do what you ask of them and let them know how to report problems.

Here are some ways to get your message across:

- Create a special website (or a section of your existing website or intranet) devoted to cybersecurity policies and education.
- Use social media to deliver messages on an ongoing basis to involved parties, keeping security in their minds.
- Have someone write a bi-weekly blog post about the company's cybersecurity initiatives.
- Create posters stressing cybersecurity best practices and hang them in employee break rooms or other places where people gather.
- Develop a classroom education program that explains your company's cybersecurity policies.
- Automatically change employee desktop wallpaper to convey security messages or warn of emerging threats.
- Promote cybersecurity awareness regularly using video training modules that employees can access from their PCs or other devices.
- Organize exercises for employees with internal fake social engineering scenarios.

Measuring Information Campaign Effectiveness

Many organizations fail at their information awareness campaigns — not because they aren't trying, but because they haven't planned and executed them correctly. Sometimes a company's solutions aren't aligned with the specific risks that an organization faces, and the company can't accurately measure the campaign's progress or value.

REMEMBER

No single metric can reveal the full spectrum of human cyber risk, so you have to look at multiple metrics when evaluating an information security awareness campaign. The metrics you use must be meaningful. Make sure they're specific, easy to interpret, and repeatable.

Awareness metrics typically measure knowledge of a specific behavior. Does the employee know what to do? These metrics are usually collected after employees complete some training, and typically this is a one-time exercise.

Possible metrics can be:

- Ability to recall the information provided during the training
- Retention of that information in different time frames, measuring awareness periodically
- Understanding of organizational and personal threats (situational awareness)

Impact metrics in a security reporting campaign assess what actually happens, not just what people know. An impact metric can tell you what your training program accomplished by looking at changed behavior.

Developing a Cybersecurity Culture

Most security awareness campaigns focus on raising awareness only. However, *people-centric security* focuses on changing security awareness, behavior, and culture in tandem. Doing so creates a virtuous circle, where improvements in one area cause improvements in another. Raising awareness creates behavior change, secure behaviors encourage a culture of security, and a culture of security further advances security awareness.

Information security culture refers to a corporate culture in which users are knowledgeable and vigilant about protecting data, information, and knowledge. Information security culture is a fundamental aspect defined by these dimensions:

- Belief in information security's importance
- Both long-term and short-term commitment to the company's information security goals, policies, procedures, and continual improvement processes
- Cooperation and collaboration among all users and IT professionals
- Ongoing auditing to make sure objectives are met
- Encouraging users to report incidents

Developing a strong information security culture can help organizations minimize many of the behavioral issues that can result in security failures. Awareness and training programs must support the organization's needs, be relevant to its culture, and consider pertinent topics.

Using multiple methods to educate users ensures that all employees have a thorough understanding of why they have to follow security policies, as well as the implications of a breach.

WARNING

A single meeting about cybersecurity is not enough to guarantee that employees understand how to keep data secure. cyberattacks come in many forms and are always evolving. An effective security culture implements changes and gets buy-in from those involved, with everyone understanding what the best practices are and what the results will be when they are — or are not — followed.

Promoting Information Security Awareness to the C-Suite

Effective cybersecurity must start with a commitment from the top of the organization. Top executives must be prepared to make the right cybersecurity investment decisions and develop effective cybersecurity strategies.

It becomes increasingly necessary for directors to have basic training in cybersecurity that addresses the strategic nature, scope, and implications of cybersecurity risk. Top management needs to provide meaningful data about not just the state of data security, but also the resilience of the organization's digital networks.

Developing a common language for management and corporate directors to discuss cybersecurity issues is also important. Digital security specialists, like all subject-area experts, must be able to communicate effectively with board members and other leaders. Information security executives must be capable of presenting information at a level and in a format that is accessible to non-technical corporate directors.

Both management and directors need to be aware of:

- **The limitations of security:** No practical cybersecurity strategy can prevent all attacks.
- **The need for resilience:** It's important to have strategies that will ensure sustainability of business during a cybersecurity breach and quick recovery in its aftermath.

REMEMBER

Networks constantly change, so tracking cyber risks and vulnerabilities over time and adapting accordingly is essential.

Involving top-level executives in a company's cybersecurity strategy also ensures that possible adverse impacts from security incidents are viewed from a bottom-line as well as from an asset-valuation perspective. For example, an organization might follow two different paths to cybersecurity effectiveness, both of which would necessarily involve top-level involvement. First, the company might add a cybersecurity expert to the board, and second, the company might assess its cybersecurity maturity against accepted standards such as the National Institute of Standards and Technology (NIST).

WARNING

Information security officers (CISOs) do not usually report to the chief executive officer (CEO) or the board. Usually security is positioned as a technical issue rather than a business concern. This reduces the scope of action effectiveness of any cybersecurity initiatives. One way an organization can boost the strength of its cybersecurity is to put a security expert in a direct line-of-business role with the authority to make cybersecurity policy decisions.

IN THIS CHAPTER

» Increasing your cybersecurity

Chapter 6
Ten Ways to Stay Cybersecure

Cybersecurity isn't a mysterious dark art — it's a disciplined set of practices that, when followed scrupulously, make an organization or individual much less vulnerable to attacks. This chapter provides a quick list of ten ways you can harden your systems to stay safer.

Protecting Networks from Attacks

Cybercriminals often look to exploit the connections between private or company networks and the Internet. You can reduce this risk by implementing policies and architectural and technical responses. The focus should be on the parts of the organization where data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Conducting Staff Awareness Training

Employees are the ones following policies and procedures, so they are directly responsible for keeping threats such as ransomware and phishing at bay. Keep them aware and educated with training

courses covering the essentials of cybersecurity and specific topics such as phishing. They should also know about the various data protection regulations such as the European Union's General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA).


TIP

One size doesn't fit all when it comes to training. Managers and those closely involved in information security should have more in-depth training courses that give them the opportunity to gain certifications.

Encrypting Sensitive Data and Emails

Data at rest or in transit should always be encrypted to prevent it from being accessed by unauthorized parties, either inside or outside the company. IT departments need to make sure that all servers store data using encryption (such as BitLocker and EFS on Windows systems, for example), and to make sure that the network protocols used to transmit data use encryption.

Using Security Utilities

Having a firewall is a first line of defense when it comes to protecting data against cyberattacks. Firewalls prevent unauthorized users from accessing websites, mail services, and other sources of information that can be accessed from the web. A company may have a hardware firewall on its internal network or may mandate that each employee computer have a software-based firewall enabled. Employees who work from home should have firewall protection as well.

Antivirus/anti-malware programs scan and remove viruses, spyware, and other malware on the computer. They also check files as they come in through email, downloads, or connected devices such as USB drives. Many antivirus/anti-malware programs have other functions too, such as preventing trackers from collecting your data and notifying you if software accesses your webcam.

Using Strong Passwords and Password Managers

Many cyberattacks happen because a thief can guess a person's password. This isn't as difficult as it sounds, especially if the password is a common word or proper name, and a variety of hacking tools are available that can run through an entire dictionary of attempts in a short time.

Strong, complex passwords that include long strings of uppercase and lowercase letters, numbers, and symbols can slow down a would-be attacker. Experts recommend passwords of at least eight characters that doesn't appear in a dictionary, isn't a proper name, and has no relationship to anything in the user's life that could be deduced from social media or online searches. It's also recommended to change passwords at regular intervals (with the exact interval depending on the sensitivity of the data being protected).


TIP

One way to create a password that is easy to remember but difficult to guess is to use a passphrase. For example, if you happen to remember your grandmother's address from childhood, you might make it into a passphrase like 720EastWarrenSt62550.

Being Careful with Email

Email is a vector for cybercrime in two main ways: malware-laden attachments and fraudulent hyperlinks. By being cautious about opening attachments and clicking links, you can avoid most email-related threats.

Employees should be trained not to open email attachments from unknown senders, no matter how tempting the filename or message may be. Many antivirus/anti-malware utilities include a feature that checks email attachments for threats as they arrive; use one of those if possible.

Avoiding Unprotected Wireless Networks

Public Wi-Fi networks may be convenient, but they also can allow hackers access to any computers that connect to them. Traveling employees should be encouraged not to use public networks, like

in airports and public buildings. If they urgently need Internet access, they can use a smartphone with a cellular data connection, or tether their laptop to a smartphone that allows connection sharing.

Wi-Fi networks in the company's offices should be secure, encrypted, and hidden. If employees are working remotely, they can help protect data by using a virtual private network (VPN). A VPN is essential when doing work outside of the office or on a business trip, and employees who travel or work remotely should be trained to connect to it and use it.

Keeping Up with Updates

Software updates are important because they often include critical patches to security vulnerabilities, they can also improve the stability of the software, and remove outdated features.

Establishing Procedures for Home and Mobile Work

Employees might work from home permanently or occasionally, or simply need access to their accounts on the go. These situations come with their own risks, and organizations need to establish policies and procedures to deal with them.

Employees need to be trained on the risks associated with remote access and advised on how to stay secure. A remote working policy needs to be developed and employees need to adhere to it.

Monitoring Compliance

Establish a monitoring strategy and produce supporting policies. System monitoring enables organizations to detect criminals' attempts to attack systems and business services. It plays a major role in detecting data breaches and helps determine whether systems are being used appropriately and in accordance with a company's policies.

Everything you need to know about cybersecurity in one place!

Cybersecurity should be an essential part of your company culture. The training of employees to be cybersecure and aware of risks is a part of that culture. In this book, cybersecurity experts Ragnar Sigurdsson and Maria Bada take you through the key elements of cybersecurity and how to maintain it at your business as well as in your home.

Inside...

- Basic cybersecurity concepts
- Understanding behavior online
- Common vulnerabilities
- Cyber-attack techniques
- Security awareness strategies
- Ten ways to stay cybersecure

awareGO

Maria Bada is a research associate at the Cambridge Cybercrime Centre and focuses on the human factor in cybercrime. **Ragnar Sigurdsson** is a former penetration tester who, through his work, discovered that people are usually the weakest link when it comes to cybersecurity. Ragnar and his wife, Helga, founded AwareGO to help organizations around the world train employees in cybersecurity awareness.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-72149-9
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.