ACT SMART I.T.
www.ACTSmartIT.com
General Business Edition — October 2024

Your Cybersecurity Awareness Plan

Every October since 2004, National Cyber Security Awareness Month, coordinated by the Department of Homeland Security (DHS), highlights the importance of cybersecurity. It aims to protect not only our identities, finances, and privacy, but also our national security, infrastructure, and economy. Everyone—from the public and private sectors to individuals—plays a role in maintaining cybersecurity.

2024 CHAMPION
CYBERSECURITY AWARENESS MONTH
ACTSmart IT is proud to be a champion!

Key Areas to Protect:

- **Personal Information**: Safeguard data that could help criminals target you.
- **Financial Resources**: This includes protecting savings accounts, assets, and credit.
- **Sensitive Data**: Keep medical records, tax information, and other private details secure.
- **Your systems and the services you use.**

The priority is to reduce risks that could lead to real-world threats. Financial security follows, as it ensures your ability to meet basic needs. Securing sensitive data is next because breaches can cause lasting damage. Last, protecting your ability to earn ensures stability for yourself and your family.

Avoiding Cyber Threats:

To prevent becoming a target of cyber threats:

- **Be Discreet Online**: Avoid showing off high-value items like cars or jewelry.
- **Limit Location Sharing**: Share specific locations only after leaving them.
- **Keep Payment Information Private**: Avoid sharing details that might reveal when you receive payments.
- **Secure Social Media Profiles**: Make your profiles accessible only to trusted individuals. Limit personal information to prevent potential attackers from gaining insight into your life.

  If your job involves access to sensitive data, be especially cautious about sharing your employer's name and your role online, including on professional sites like LinkedIn.

Strengthening Financial Security:

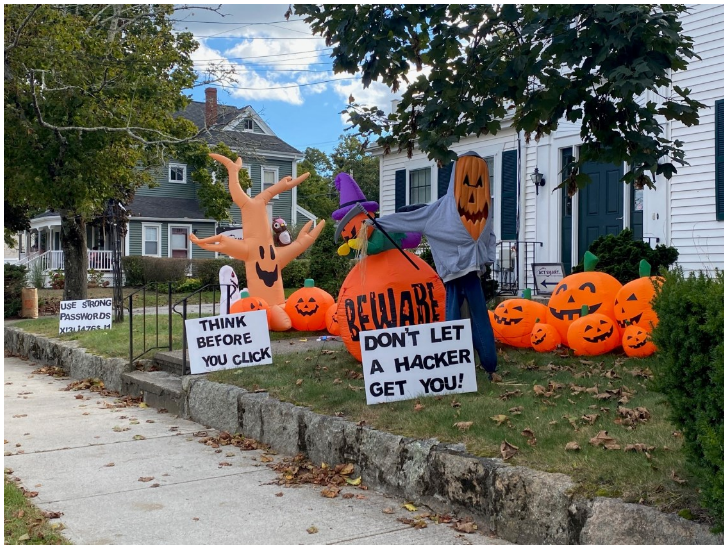
- **Audit Your Accounts**: List all savings and investment accounts and understand how identity verification works for each. Know what information a potential attacker would need.
- **Implement Extra Security Measures**: Use bank-offered features like two-factor authentication, callback confirmations, and real-time transaction alerts.
- **Regularly Monitor Accounts**: Review account activity weekly for any unauthorized transactions.
- **Freeze Your Credit Report**: Restrict access to prevent identity thieves from opening accounts in your name.

Continued on page 3

From The Desk of David Snell

Happy October, or as Pam says, "Happy Cybersecurity Awareness Month!"

We're proud that we have been National Cybersecurity Awareness Champions for about ten years. StaySafeOnline.org, the National Cybersecurity Alliance has been a wonderful resource for security articles and information..



Pam even made the front lawn at the office lessons in cybersecurity. We've entered into the local Scarecrow Contest with security theme.

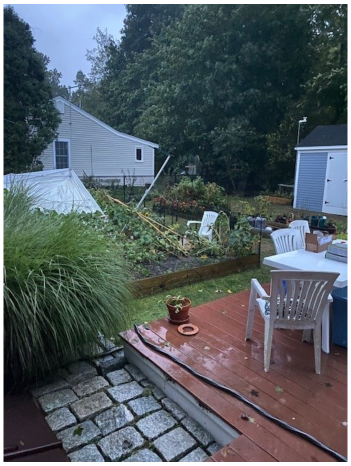
I think the information in our front page article is great advice. It's a little bit different take on updating your Cybersecurity plan.

I do want to add that on a recent radio spot on 95.9 WATD, I reported on NIST's newest passwords guidelines. (https://actsmartit.com/nist-password-guidelines) You may be pleasantly surprised by their new approach to password security. We'll see how quickly the banks and other password-protected sites adapt to their suggestions.

We used information that they provided for our article on pages 4 and 5: "**Stay Alert: Credit Card Skimming Can Happen Anytime."** We hear too much about credit card skimming at supermarkets and gas stations in our area.

We're also reporting on a recent update to PayPal's Terms of Service. Starting Nov. 27, PayPal will share your purchasing data with third-party merchants. We've got instructions to allow you to opt out of their scheme. You can read the article from our friend Caitlyn, of Computer Services Unlimited in Virginia, for the instructions to opt out on page 6.

The Grammar Goddess, Susan Rooks, has agreed to contribute a monthly article on LinkedIn basics for all users. Her article on page 7 tells of how she learned to Stand Out on LinkedIn. Even if you've been a longtime LinkedIn user, you'll find information to help you improve your standing. I'll be updating my LinkedIn profile this month!



I usually end my monthly letter by talking about my garden. It was a very good growing year, until a sudden windstorm in September took the canopy off our deck and threw it into the garden! It looked like a giant white spider with its legs up in the air after it smashed down on my bean and

cucumber trellises. It hit a few tomato plants, too. I was able to harvest what was left on the vines; those cukes were so good and we miss having them with dinner every night!

I'm looking forward to next year's garden!

Happy Halloween!

Your Cybersecurity Awareness Plan (Continued from front page)

Protecting Sensitive Data:

Sensitive data includes medical records, tax returns, and social security numbers. To protect this information:

- **Minimize Data Creation**: Only provide per sonal information when absolutely necessary.
- **Delete Unnecessary Data**: Regularly delete old data that could be sensitive, ensuring it's permanently removed from devices.
- **Use Encryption**: Encrypt your hard drives and password-protect devices like phones, tablets, and laptops.

Keep your systems and the services you use secure:

- **Use Strong Passwords**: A password manager can help generate unique passwords for each site, reducing risks if one account is compromised. (See new guidelines from NIST at https://actsmartit.com/nist-password-guidelines)
- **Secure Your Devices**: Use disk encryption on computers and strong passwords on all devices.
- **Be Careful with Data**: Only store and share information when necessary, and delete what is no longer needed.
- **Enable Two-Factor Authentication**: Add an extra layer of security to all accounts.
- **Securely Store Backup Drives**: Keep them in a safe place and securely erase data when no longer needed.

Maintaining Online Integrity:

- **Read Before Sharing**: On social media, always read and understand what you share to avoid inadvertently spreading misinformation.
- **Protect Social Media Accounts**: If compromised, an account could be used for spam, damaging your online reputation.
- **Safeguard Websites**: Keep your website secure to prevent hackers from damaging your site and harming your reputation with customers.
- **Secure Email Accounts**: An insecure email account can lead to phishing attacks on your contacts, harming your reputation and potentially theirs.

Caution with Apps:

Be Selective with App Permissions: Avoid granting access to your contacts list or other sensitive information unnecessarily.

By focusing on these areas, you can play your part in making the digital world safer—not only for yourself but for the broader community. National Cyber Security Awareness Month serves as an annual reminder of these principles, encouraging everyone to adopt habits that strengthen their digital defenses and contribute to a secure online environment for all.

Stay Alert: Credit Card Skimming

It's a normal day—you're filling up at the gas station or withdrawing cash from an ATM. But unbeknownst to you, criminals may be capturing your credit card information, leading to unauthorized transactions that can drain your finances. While technology evolves to make cards safer, scammers adapt to exploit any gaps. Staying informed and vigilant is your best defense against these ever-changing threats.

What Is a Credit Card Skimmer?

A credit card skimmer is a device used by criminals to steal card information by secretly recording data from the magnetic stripe of a swiped or inserted card. As EMV chip cards become standard, criminals have turned their attention to places where magnetic stripe transactions still occur, like certain ATMs or gas station terminals. This shift has led to a new threat: *shimming* devices, which focus on capturing information from EMV chips.

Modern skimmers have also advanced. Some now use Bluetooth or other wireless technologies to transmit stolen data, reducing the chances of their detection. These devices can even record your PIN, making them a threat at pay-at-the-pump stations, where the adoption of chip readers has lagged behind.

What Happens When Your Card Is Skimmed?

When criminals skim your card, they capture its details and use that information to make unauthorized purchases, create cloned cards, or commit identity theft. If a debit card is targeted, scammers could drain your bank account. If they gain access to additional personal information, such as through data breaches or phishing, they might access other accounts, causing even more significant damage.

Understanding Card Shimmers

Shimmers are smaller and more discreet than traditional skimmers. These devices are inserted directly into the chip card reader slot, making them hard to detect. They work by intercepting and recording information from your card's chip. While traditional skimmers are often external attachments, shimmers hide inside the card reader. With the stolen information, scammers can create counterfeit cards or make unauthorized transactions.

Types of Credit Card Skimmers

Criminals use various skimmers to steal card information. Here are the most common types:

- **Overlay Skimmers**: These devices fit seamlessly over the existing card slot.
- **Insert Skimmers**: These are hidden inside the card reader's slot.
- **Insert Shimmers**: Target the EMV chip cards by fitting into the chip card slot.
- **Wiretap Skimmers**: Intercept data transmissions within the device.
- **Bluetooth Skimmers**: Enable wireless transmission of stolen data.
- **Miniaturized Skimmers**: Concealed within or discreetly attached to the card reader.

How to Protect Yourself Against Skimming and Shimming

Since skimmers are designed to blend in, it's essential to be proactive when using your cards. Here are some tips to protect yourself:

- **Avoid Suspicious Pay Terminals**: Use card readers in well-lit, high-traffic areas, even though criminals occasionally target large chains.
- **Inspect Card Readers**: Check for signs of tampering, such as loose parts, jiggly components, or unusual protrusions.
- **Cover the Keypad**: When entering your PIN, cover the keypad to prevent hidden cameras from capturing it.

Can Happen Anytime

- **Use Chip-Enabled Cards**: They are more secure than magnetic stripe cards, even though they can still be at risk from shimmers.
- **Opt for Contactless Payments**: Tap-to-pay technology eliminates the risk of skimming and shimming.
- **Monitor Account Activity**: Regularly review your accounts and report any suspicious transactions.
- **Use Digital Wallets**: Mobile payment apps provide extra security through tokenization. Stick with trusted services like Apple Wallet or Google Pay.
- **Prefer Credit Cards Over Debit Cards**: If your card is skimmed, disputing fraudulent charges is often easier with credit cards than recovering funds taken directly from a checking account.

Understanding Chip Credit Cards

Chip-enabled cards are designed to be more secure than magnetic stripe cards. They contain an encrypted microchip that stores and transmits your card information. Each time you use a chip card, it generates a unique transaction code, which makes it difficult for scammers to duplicate the card.

While chip cards significantly reduce the risk of cloning, they are still vulnerable to card-not-present fraud—where scammers use stolen data for online purchases. However, their introduction has substantially decreased cases of skimming at physical terminals.

What You Should Know About Tap-to-Pay Technology

Tap-to-pay, or contactless payment, uses near-field communication (NFC) to securely transmit payment data from a card or smartphone to a payment terminal. The data is encrypted, making it very difficult for criminals to intercept. While there have been isolated cases of scammers using NFC readers to attempt skimming, security features like transaction limits and authentication help minimize this risk.

Continuous improvements in encryption and tokenization have made tap-to-pay a safe and convenient option for transactions. Using contactless payments helps consumers protect their data without sacrificing convenience.

What to Do If You're a Victim of Skimming or Shimming

If you suspect that your card information has been skimmed or compromised, take immediate action:

- **Contact Your Bank or Card Provider**: Report any unauthorized transactions and request a freeze or cancellation of your card. They can guide you through the dispute process and issue a replacement.
- **Monitor Account Activity**: Keep a close eye on your statements for any further suspicious activity.
- **Freeze Your Credit**: This step can prevent identity theft. You can unfreeze your credit when you need to apply for a loan.
- **Strengthen Passwords and Use Multi-Factor Authentication**: Ensure that all accounts have unique, strong passwords and enable extra security layers.

If your personal data has been compromised beyond your card details, notify relevant authorities and credit bureaus to report potential identity theft and explore options for further protection.

Vigilance Is the Best Defense

Being aware of where you use your credit or debit card is critical, but so is routinely reviewing your financial statements and credit reports. Sign up for account alerts or notifications to keep track of real-time activity. Staying informed about common scams and keeping an eye out for suspicious transactions can make a huge difference.

By maintaining this vigilance, you can not only catch potential instances of card skimming but also stay alert for any other forms of fraud that might target you. While technology will continue to improve, so too will the tactics of scammers—staying one step ahead is up to you.

Resource: https://staysafeonline.org/resources/protect-your-credit-cards-from-skimmers-and-shimmers/

Protect Your Privacy: Important PayPal Update

Starting November 27, 2024, PayPal will start implementing new terms and conditions that users should be aware of, especially concerning privacy and data sharing.

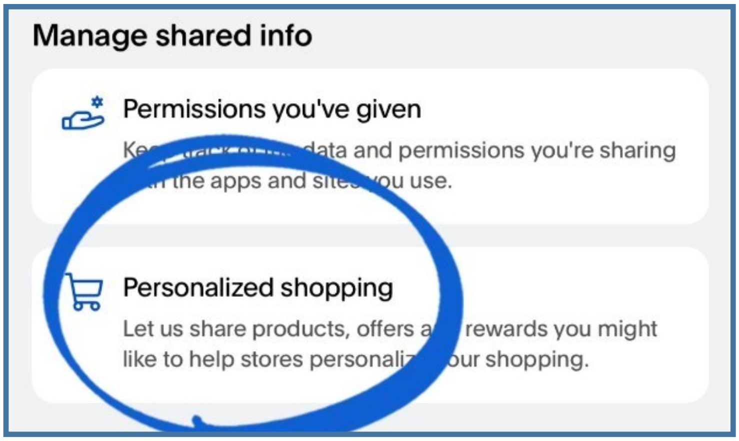
The company is making a gradual shift toward leveraging user information to create personalized shopping experiences." While this can enhance your shopping journey, it raises important questions about the security of your personal data.

Under the new terms, PayPal may disclose personal information including your product preferences, sizes, and styles to provide tailored recommendations. This may seem beneficial for creating a more customized experience, but if there's any concern about safeguarding your personal information on PayPal, here are some steps you can take to protect yourself:

1. **Access Your Settings**: Log in to your PayPal account app and click on your profile icon.

2. **Navigate to Data & Privacy**: From the settings menu, select the "Data & Privacy" option.

3. **Manage Personalized Shopping**: Find the section labeled "Personalized Shopping."



Manage shared info

Permissions you've given

Keep track of the data and permissions you're sharing with the apps and sites you use.

Personalized shopping

Let us share products, offers and rewards you might like to help stores personalize your shopping.

4. **Toggle Off Personalization**: Switch the toggle off to secure your data.

By taking this action, PayPal assures users that they will only disclose your personal information as necessary to complete transactions you initiate. This means your data will not be shared with partners and merchants for the purpose of creating personalized shopping experiences.

Additional Steps to Enhance Your Privacy

In addition to managing your personalized shopping settings, consider these extra steps to further protect your information on PayPal:

- **Review Privacy Settings Regularly**: Make it a habit to check your privacy settings periodically to ensure they align with your preferences.

- **Monitor Transactions**: Keep an eye on your account activity for any unauthorized transactions and report them immediately.

- **Use Strong Passwords**: Create strong, unique passwords for your PayPal account and consider enabling two-factor authentication for an added layer of security.

- **Limit Connected Apps**: Review any third-party applications linked to your PayPal account and disconnect those that you no longer use or trust.

While PayPal's shift towards personalized shopping experiences could enhance convenience, it's essential to stay vigilant about your privacy. By understanding the new terms and taking proactive steps to manage your data, you can enjoy the benefits of PayPal while maintaining control over your personal information.

Visit ***https://www.paypal.com/us/legalhub/upcoming-policies-full*** to find more information. Make sure to stay informed and adjust your settings to fit your privacy preferences!

Thanks to our colleague, Caitlyn, of CSUinc.com in Virginia for this article.

LinkedIn™: How to stand out from the crowd

You've all heard of LinkedIn, right? It's the go-to business platform for a lot of business folks worldwide, whether they work for others or themselves.

But how successful are most of them in getting what they'd hoped for – usually clients?

Not very.

As with most new ventures, it takes a lot of knowledge to figure out the ups and downs, rights and wrongs of using LI to succeed in getting what we want out of it.

LI officially launched in 2003, and I joined in October 2005, when it was just beginning to be a sought-out venue. But there weren't many folks using it then that I knew, so I did what I could for about 10 years, although I really didn't know how to make the most of it.

I was actually thinking of quitting it because it was so much work with very little to show for it.

But I got lucky because a couple of wonderful folks saw my posts and showed me how to do far better than I was doing on my own.

Fast-forward to today: I know how to help others maximize their presence, find clients, learn from others, and use their time on LI to great advantage. And given that right now in 2024, there are an estimated 1 BILLION profiles on the platform, it definitely pays off to understand how to make it all work. (It's also estimated that about ¼ of that billion actually use LI, but that's still a lot of people!)

In this series of articles, I'll cover the sections of any LI profile, showing you exactly how to create them to help YOU stand out from the crowd and rise above the noise.

The 5 major sections are:

The **banner**, that space at the top that LI fills with a gray or green "nothing much" background.

The **picture**, which should be one of **us** that invites others to get to know us.

The **headline**, the first few words under our picture, which should give a hint of what we do and why it matters.

The **About** section, which gives us room for 2600 characters, including spaces, to describe how we help others.

The **Featured** section, which we can use to show some of our own favorite articles that aren't easily found on our profile.

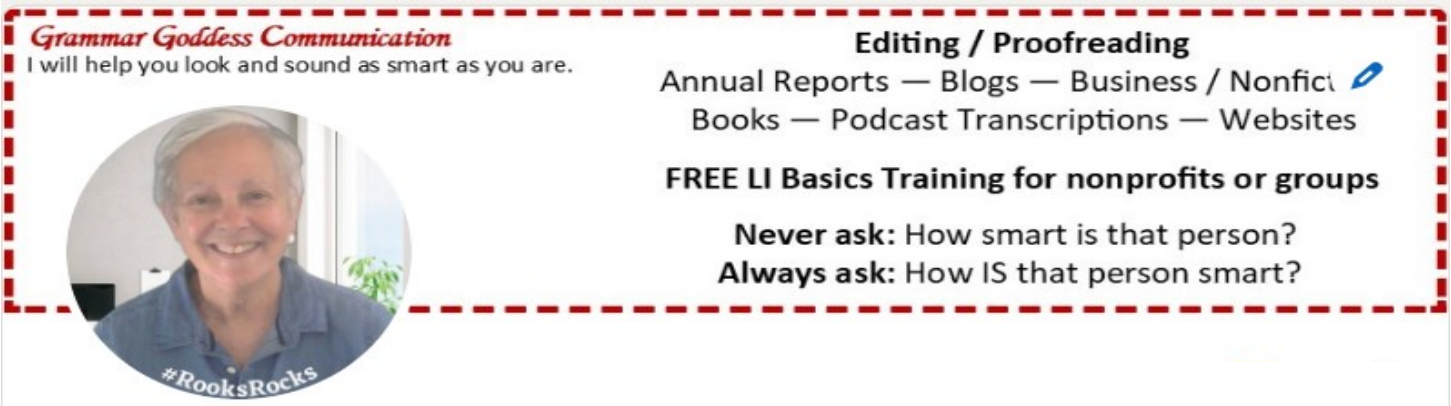
Too many folks skip over these, but they're the FIRST things anyone sees. They can make or break someone's decision to keep reading to see who we are and what we do that might help them.

Now, I know that many who are reading this think they don't need or want LI because their company largely gets its clients only in local areas.

But, think of this: A friend of yours lives 1,000 miles away but sees something you wrote that is EXACTLY what a friend of theirs is looking for, and that person lives just 20 miles away from you!

So while LinkedIn may not be for everyone, it's still worth exploring to see exactly how it could be for YOU. Feel free to check out my profile (https://www.linkedin.com/in/susanrooks-the-grammar-goddess/) and others, and see if anything we've done gives you some ideas for your own profile.

Next month, I'll show you exactly how to create your banner, with some great examples that I love.



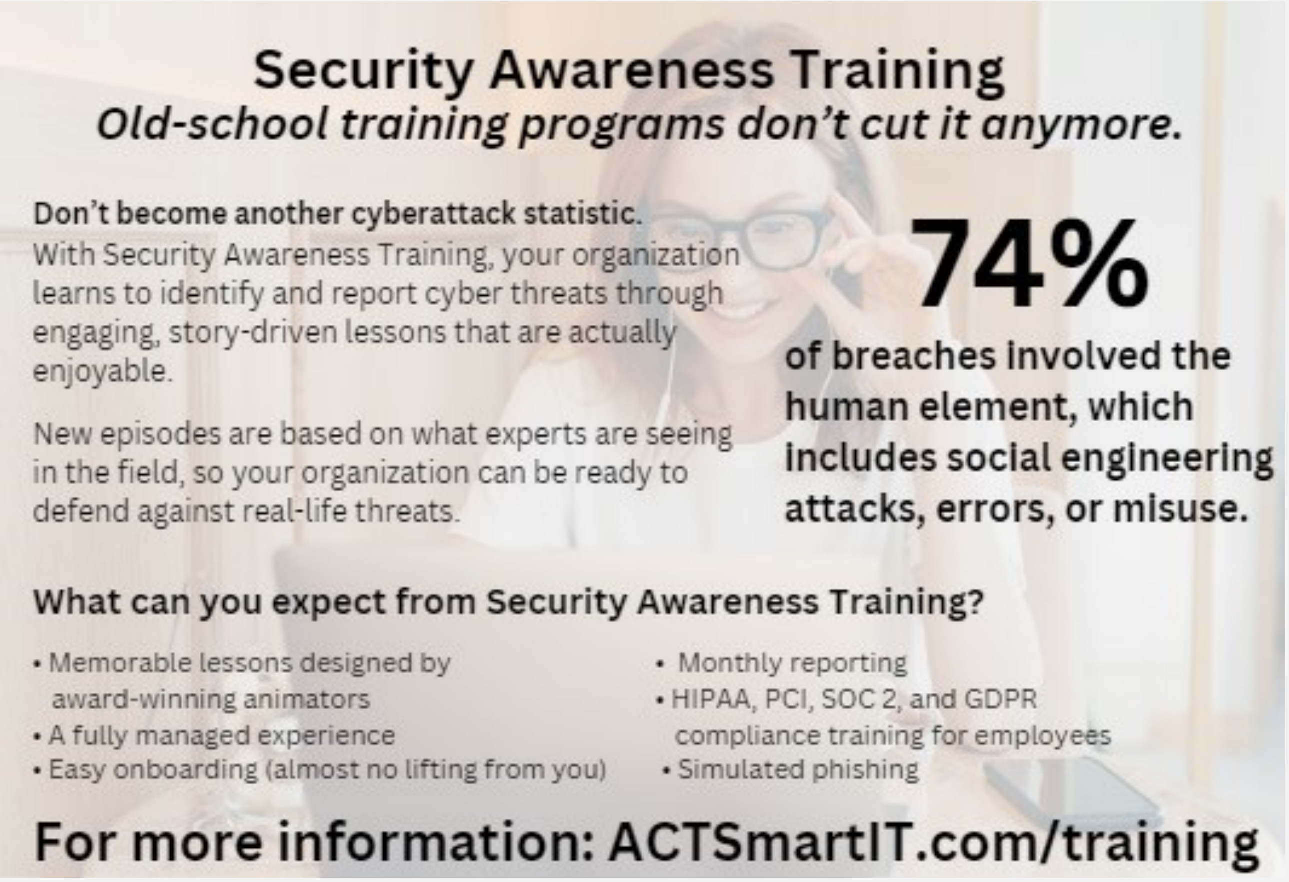
ACTSmart IT
332 Main Street
Wareham, MA 02571

ACT SMART I.T.
www.ACTSmartIT.com

In This Issue:

This newsletter was thoughtfully edited by
Susan Rooks, the Grammar Goddess,
so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
508 272-5120
SusanR@GrammarGoddess.com



Security Awareness Training

Old-school training programs don't cut it anymore.

Don't become another cyberattack statistic.
With Security Awareness Training, your organization learns to identify and report cyber threats through engaging, story-driven lessons that are actually enjoyable.

New episodes are based on what experts are seeing in the field, so your organization can be ready to defend against real-life threats.

74%

of breaches involved the human element, which includes social engineering attacks, errors, or misuse.

What can you expect from Security Awareness Training?

- Memorable lessons designed by award-winning animators
- A fully managed experience
- Easy onboarding (almost no lifting from you)
- Monthly reporting
- HIPAA, PCI, SOC 2, and GDPR compliance training for employees
- Simulated phishing

For more information: ACTSmartIT.com/training