



Protecting Your Business From New Devices and Cyberthreats After the Holidays

December is here! Between Black Friday and Christmas each year, we witness the influx of holiday-gifted devices and their smiling owners. (We enjoy these fun grownup “toys” just like everyone else.) Before too long, your employees will settle back into the office and bring new devices they want to connect or use for work.

Welcome to the world of BYOD (Bring Your Own Devices).

Smartphones, laptops, and tablets are always popular holiday gifts, but let’s call them what they are to your company: foreign machines invading private networks. Attackers love unsecured devices.

Most of these new devices come loaded with unsanctioned software and apps that, if you’re not careful, can introduce new threats to your network, like viruses, spyware, and ransomware.

Key BYOD Security Risks

BYOD can present a security risk since personal devices may not have the same security controls as company-provided devices.

The main security risks of BYOD include:

Lost or stolen devices: Personal devices can be easily misplaced or stolen, potentially exposing sensitive company data to unauthorized individuals.



From The Desk of David Snell

December 2024!

If you, your family, or your employees have asked Santa for new electronic devices for Christmas, be sure to read our front page article **"Protecting Your Business From New Devices and Cyberthreats After the Holidays."**

While anyone receiving these gifts may be excited, they also need to take precautions as they use them at home or in the office.

Our friend Vinny Pircio, Branch Manager of the Rockland Trust in East Wareham, gives us information on one of the many scams that customers fall prey to. **"The Romance Scam"** can quickly wipe out the victim's savings and more!

Attorney Helen Horn Figman has given us an **"IMPORTANT UPDATE TO REQUIREMENTS UNDER THE MASSACHUSETTS PAID FAMILY AND MEDICAL LEAVE ACT AND SALARY LEVEL FOR HOURLY VS. SALARY ANALYSIS"** You'll find that on page 6. When it comes to money, EVERYONE wants to know!

Our editor and good friend Susan Rooks, the Grammar Goddess, is continuing her series on LinkedIn with this installment about LinkedIn Headlines. It's on page 7.

Finally, take a look at the back page notice for FREE Security Awareness Training. Our security partner, Huntress, has made 9 episodes available to ANYONE. No cost or obligation; we don't even get a list of who is taking advantage of these fun learning games. Let us know what you think.

Once again, we're *Grinched Up* for the holidays!



Even though he didn't contribute an article to this newsletter, you can find his newest scam that he loves, "Chinese Organized Crime and Gift Card Fraud." What better way to make someone miserable than to steal the money off a gift card before it gets to the recipient! You can find the whole story at **ACTSmartIT.com/ginch-gift-card-scam**

This year, Pam added CindyLou Who to keep him in line!

Pam Dziura from the Cranberry Country Chamber stopped by with their Chamber Elf Berry. Berry had fun playing with all our Grinch decorations, checked out the WOW treats that we bring to clients and even spent some time looking at our website and the Chamber's.

Happy Holidays from the ACTSmart Team!



David Snell

Malware and unauthorized applications:

Employees may unknowingly download malicious software or use unauthorized applications that can compromise the security of company resources.

Unsecured networks: Employees often connect to public WiFi networks, which are vulnerable to hackers and eavesdropping and pose a significant risk to BYOD security.

Data leakage: Employees can unknowingly download malicious third-party apps that hackers can control or inadvertently share sensitive information through unsecured channels, such as personal email or cloud storage accounts.

Unclear security policies: Employees may not be aware of the risks and may bypass company data security policies on their devices, putting the network at risk.

A BYOD policy is essential, no matter the size of your company.

***Note:** Before we list some tips and best practices for a BYOD policy, we need to say that we're not lawyers, nor do we play one on TV. If you don't already have a BYOD policy, we can help you outline policies that will fit your company. However, we still recommend that your attorney review your BYOD policy to ensure you and your employees are legally covered.

1. Regular Device Audits

Regularly audit registered devices to ensure compliance with security policies and identify potential vulnerabilities, which includes checking for the latest operating system updates, verifying the presence of security software, and confirming the absence of unauthorized applications.

2. Mandatory Security Software

Require employees to install and maintain up-to-date security software on their personal devices, including antivirus software, firewalls, and anti-malware solutions. Regularly update these security tools to protect against emerging threats.

3. Mobile Device Management (MDM)

Using an MDM tool/software ensures that each BYOD device meets minimum security standards and is configured to access corporate resources. Most MDM tools can remotely lock devices or erase company data if a device is lost or stolen.

4. VPNs and Encrypted WiFi

Encourage the use of Virtual Private Networks (VPNs) when accessing company resources from outside the office. VPNs encrypt internet traffic, providing a secure connection to the corporate network. Additionally, employees should be educated about the importance of connecting to encrypted WiFi networks to prevent unauthorized access.

5. Clear Employee Expectations

Communicate expectations regarding the use of personal devices for work-related activities. Employees should be aware of their responsibilities to protect company data, promptly report security incidents, and adhere to the organization's BYOD policy.

6. Strong Authentication Measures

Implement strong authentication measures, such as multi-factor (MFA) or biometric authentication, to ensure only authorized individuals can access company resources. Doing so adds an extra layer of security, even if a device is lost or stolen.

7. Employ Least Privilege Access Control

Adopt the principle of least privilege, granting employees access only to the resources necessary to perform their job duties. Doing this reduces the risk of unauthorized access and limits the potential impact of a security breach.

If you are in a regulated industry (Finance, Health Care, Law, etc.) and your employees use their own personal devices, you must have a BYOD policy! Your business has legal and regulatory requirements that apply to company data and operations (e.g., HIPAA, GDPR, NIST, SOC 2). A good BYOD policy helps with compliance and reduces the risk of data breaches and leaks.

If you would like assistance reviewing, updating, or creating a BYOD policy, call us, and we'll be happy to help.

The Romance Scam

So much of our lives are digital, and with more and more of our banking being done electronically it is more important than EVER to make sure you don't become a victim of fraud. This month, we are going to learn about a scam that can unfortunately be a challenge to identify. This scam is what we call the "Romance Scam."

In today's connected world, online relationships have become increasingly common. While many find love or friendship through digital platforms, others fall victim to a more sinister reality — romance scams.

These deceptive schemes prey on people's emotions, manipulating them into sending money or personal information to scammers posing as romantic partners.

With the rise of social media, dating apps, and messaging services, romance scams have become more sophisticated and widespread, often leaving victims heartbroken and financially devastated. In this article, we'll explore how romance scams work, how to recognize the warning signs, and what steps you can take to protect yourself from falling prey to these dangerous frauds.

A romance scam typically unfolds in several stages, with scammers employing manipulation and deceit to build trust and exploit emotions.

The scam starts when the fraudster makes contact, often through social media, dating apps, or online platforms. The scammer creates a fake profile, usually using stolen or stock photos of attractive individuals. They might claim to be living overseas, often in a military or business-related profession. Once contact is made, the scammer quickly establishes a deep emotional connection.

They may shower the victim with compliments or attention. The goal is to make the victim feel needed and emotionally invested. This stage may take weeks or even months, with frequent messaging to maintain the illusion of a genuine relationship.

The scammer will slowly share a fabricated story to deepen the emotional connection, often involving an urgent or dire situation requiring financial help. For example, they might claim to be stranded in a foreign country due to an emergency, have an urgent medical issue, or face a



sudden legal or financial crisis. They exploit the victim's feelings of sympathy and affection, encouraging them to offer help. After building trust, the scammer will eventually directly request money.

This might start small, with an excuse like needing help with travel expenses, medical bills, or a visa application fee. As the victim sends money, the requests will become more frequent and significant. They may make the victim feel guilty for not sending money, claim their love is real, or even threaten to end the relationship if the victim doesn't comply.

The emotional pressure builds, making it harder for the victim to see the situation clearly. At this point, the scammer might isolate the victim from family and friends, claiming they're the only person who truly understands them. The victim might be discouraged from sharing their concerns or requests for advice with others, as the scammer may assert that no one else would understand their unique bond.

In other cases, they may continue the scam indefinitely, constantly coming up with new emergencies to extract money. For many victims, the aftermath is not just emotional but also financial. They may lose large sums of money, sometimes over months or even years. Sometimes, the scammer might disappear completely, leaving the victim feeling embarrassed and devastated.

Reporting the scam can be difficult, as scammers often operate from overseas, making legal action nearly impossible. Understanding how romance scams operate can help individuals recognize the signs early on and avoid falling into these traps.

Protecting yourself from a romance scam involves being vigilant and aware of the red flags commonly associated with fraudulent schemes. Here are the key steps you can take to protect yourself:

1. Be Cautious of Unsolicited Contact

- If someone contacts you online or through social media platforms and claims to have romantic interests without prior interaction, be cautious. Romance scammers often target people through dating apps, social media, or even email.
- Scammers often use profiles with fake photos and fabricated backstories.

2. Watch for Red Flags in Communication

- **Too good to be true:** If the person seems perfect, too attractive, or too interested in you too quickly, it's worth questioning their intentions.
- **Fast-moving relationship:** Scammers often try to quickly establish a deep emotional connection to manipulate you.
- **Requests for money or gifts:** One of the most common signs of a romance scam is when the person asks for money, particularly under urgent circumstances like a medical emergency, travel issue, or financial crisis.

3. Verify Their Identity

- **Reverse image search:** Use a tool like Google's Reverse Image Search to check if their photos appear elsewhere on the internet, which could indicate they're using a stolen or fake identity.
- **Video calls:** If they refuse to have a video call or always have excuses, it's a red flag. Scammers often avoid face-to-face communication.

4. Consult Trusted Friends or Family

- If you're unsure about someone you're interacting with, talk to a friend, family member, or someone you trust about your concerns. They can often help you see things from a different perspective and spot potential scams you may have missed.

By staying alert to these warning signs and exercising caution, you can protect yourself from falling victim to romance scams.



Vincent A. Pircio, Branch Manager II

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

IMPORTANT UPDATE

IMPORTANT UPDATE TO REQUIREMENTS UNDER THE MASSACHUSETTS PAID FAMILY AND MEDICAL LEAVE ACT AND SALARY LEVEL FOR HOURLY VS. SALARY ANALYSIS

No Accrual Of Benefits Required While On PFML

Recently, the Massachusetts Supreme Judicial Court ruled that the Massachusetts Paid Family and Medical Leave Act does not require that employees be allowed to continue to accrue benefits such as vacation, sick leave, and length-of-service credit while on PFML.

What should you do in response to this change? It's time to review your leave policies. Let's make sure that your leave policies are up to date and clearly define the rights of the employee as well as the obligations of your business during this leave. Employers may choose to continue to provide such benefit accrual (may be easier administratively), but they are no longer required to do so.

Communicate with Employees

As always, clear communication with your employees is key for effective employee relations. When you become aware that an employee has applied for PFML, take the initiative to inform him/her/them what benefits will and will not accrue during their absence. This timely transparency can help avoid misunderstandings and even potential legal actions.

ALSO, employees should be informed (at the inception of the leave) that they are responsible for maintaining their share of the monthly health insurance premium, if applicable.

Salary versus Hourly

A November 15 federal court decision has struck down the salary level increase scheduled for January 1, 2025. In addition, the July 1 increase that most employers have already implemented has also been struck down. Subsequently, going forward, employers are back to the 2019 salary test applied to exempt / salaried employees, which is \$684.00 per week. Key factors to the hourly versus salary analysis are the nature of the duties performed in the executive, administrative and professional exemption categories.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.



Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

LinkedIn Headlines

So far in this series, we've learned more about using LinkedIn™ to draw others to our profile with information on the **banner** and the **picture**.

Now comes the **Headline**, the words right under your name that explain a little bit about who we are and why anyone should care about what we do.

Always start with the **most important** idea. What do you want others to see first?

We have 220 characters, including spaces. Use a separator between ideas, like a comma, a | or *, or even an emoji.



Sarah Elkins (She/Her) · 1st
International Speaker | Workshop Facilitator | Storyteller | Musician | Gallup StrengthsFinder Coach | 300+ Episodes Podcast Host | Author | Job Interview Coach
Helena, Montana, United States · [Contact info](#)

Of course, you may also see this kind of "Headline," which is terribly easy to just skip over ...

I blocked out the phone number (& name) that had been listed ... but there's no reason to even call it, right?

With something like 1 billion profiles on LI, we really need stand out above the noise!

And remember: You can always change your details in any section of your profile at any time — and many of us do that regularly.

The Extra Value of a Headline

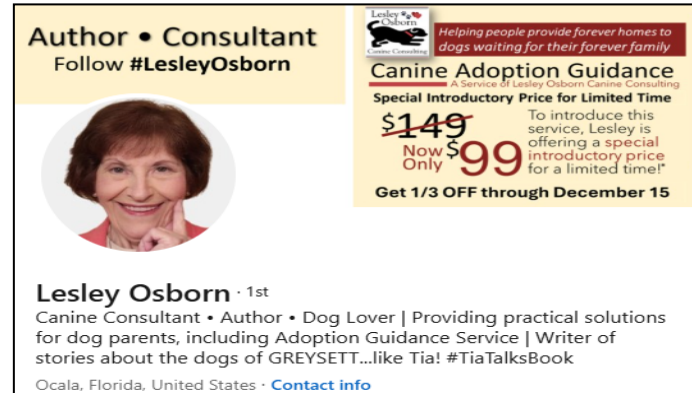
When you repost / share an article, notice what others will see immediately – yes!

The first line of your headlines.

Therefore, readers can decide quickly who you both are.

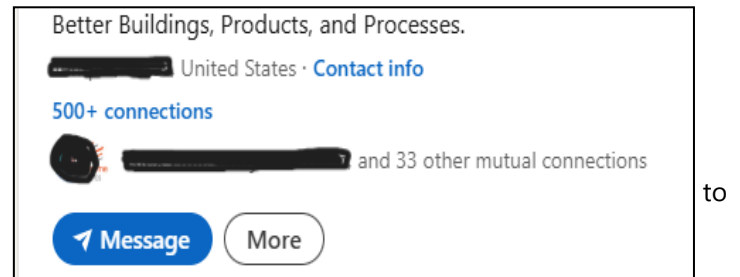
Remember: It's well worth the time you can spend looking closely at others' profiles, especially their headlines. You never know where and when you'll see something you could use on your own!

Next month, we'll explore the next section – the **About** section.. And I'm open to any questions you may have.

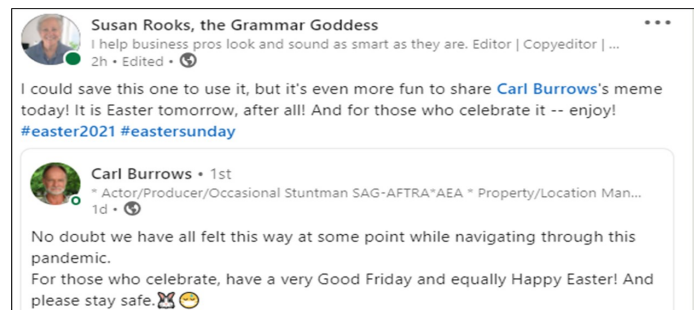


Author • Consultant
Follow #LesleyOsborn
Lesley Osborn · 1st
Canine Consultant • Author • Dog Lover | Providing practical solutions for dog parents, including Adoption Guidance Service | Writer of stories about the dogs of GREYSETT...like Tia! #TiaTalksBook
Ocala, Florida, United States · [Contact info](#)

Helping people provide forever homes to dogs waiting for their forever family
Canine Adoption Guidance
A Service By Lesley Osborn Canine Consulting
Special Introductory Price for Limited Time
~~\$149~~
Now Only \$99
To introduce this service, Lesley is offering a special introductory price for a limited time!
Get 1/3 OFF through December 15



Better Buildings, Products, and Processes.
United States · [Contact info](#)
500+ connections
and 33 other mutual connections
[Message](#) [More](#)



Susan Rooks, the Grammar Goddess
I help business pros look and sound as smart as they are. Editor | Copyeditor | ...
2h · Edited · 🗨️

I could save this one to use it, but it's even more fun to share **Carl Burrows's** meme today! It is Easter tomorrow, after all! And for those who celebrate it -- enjoy!
[#easter2021](#) [#eastersunday](#)

Carl Burrows · 1st
* Actor/Producer/Occasional Stuntman SAG-AFTRA*AEA * Property/Location Man...
1d · 🗨️

No doubt we have all felt this way at some point while navigating through this pandemic.
For those who celebrate, have a very Good Friday and equally Happy Easter! And please stay safe. 🙏🏻🙏🏻

Grammar Goddess Communication

I will help you look and sound as smart as you are.



Editing / Proofreading of
Annual Reports — Blogs — Business / Nonfiction
Books — Podcast Transcriptions — Websites

Never ask: How smart is that person?
Always ask: How IS that person smart?

In This December, 2024 Issue:

- **Protecting Your Business From New Devices and Cyberthreats After the Holidays**
- **Romance Scams**
- **Important Legal Update**
- **LinkedIn Headlines**
- **And MORE!**

«First Name» «Last Name»

«Company»

«Billing Address Line 1»

«Billing Address City», «Billing Address State» «Billing Address Postal Code»

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

LinkedIn: www.Linkedin.com/in/SusanRooks-the-grammargoddess/

Spread Holiday Cheer, Not Cyber Fears!

FREE Security Training!

For Employees, Family & Friends!



The holiday season is here, and we know it's a time filled with joy, shopping, and travel. But while you're spreading cheer, cybercriminals are on the lookout for new opportunities to strike.

That's why we've partnered with Huntress to offer free security awareness training to help you stay safe this season. Step into the Curriculaville Universe, where hackers like Deedee are up to no good – but don't worry: their fellow citizens are ready to show you how to stop them!

You'll learn practical tips to protect yourself from holiday cyber threats, so you can focus on what truly matters: celebrating with loved ones.

For your links to access these 9 trainings, go to:

ACTSmartIT.com/gift

Feel free to share. We don't have access to any email addresses used. Available through December 31, 2024