Newsletter: June 2023

BACK TO THE SECURITY BASICS

An update and review of important cybersecurity topics

THIS MONTH'S TOPICS:

Ransomware

6 tips to handle new tactics

Device Compromise

The rise of mobile devices targeted...

Scam of the Month:

BEC Scams and SLAM method...

Monthly Mashup:

June updates and review...

This month we are going back to the basics! Reviewing key topics and staying up to date on cybersecurity changes can make all the difference in your educational journey.

The cybersecurity world is constantly finding ways to thwart a cybercriminal's attack. But as we start to understand their tactics, cybercriminals then adapt their old tricks to fit the new digital world we live in.

In this month's newsletter, learn how cybercriminals are changing up ransomware attacks, account takeovers, and BEC scams.

6 Tips to Avoid and Handle Ransomware

As the regulation and prevention of ransomware attacks improve, cybercriminals are finding new ways to carry out attacks. One change over the years is the price of not paying the ransom. This used to lead to data and files being lost. But now on top of that, it often leads to confidential information being leaked to the public. While this can seem daunting, there are still ways end-users can avoid and respond to ransomware.

1 Avoid clicking links in emails. Go to websites directly instead. Clicking malicious links could lead to ransomware.

2 Use multi-factor authentication and long, unique passwords.

3 Update software on time in order to implement security patches.

4 Get familiar with your company's ransomware response plan.

5 Backup data so it's not lost if an attack occurs.

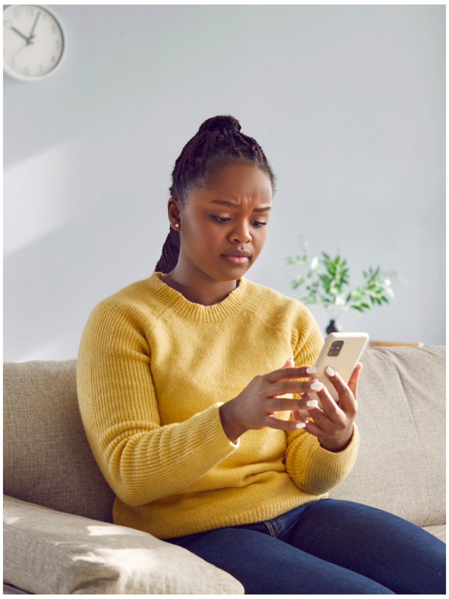
6 If an attack occurs, unplug devices so they disconnect from the internet and the network.

HOW TO SPOT AND RECOVER FROM

MOBILE DEVICE COMPROMISE

SPOT IT

- Your passwords or account details have been changed.
- Unknown apps are appearing randomly on your device.
- Your device is slower than normal.



HOW TO HANDLE MOBILE DEVICE COMPROMISE

Mobile device compromise can start with a compromised email or social media account, a malicious app, or a malicious website or link. No matter what the method of compromise, make sure to alert your contacts. If your mobile device is used for work, notify your organization, as well. Only keep work files and apps on mobile devices if absolutely necessary.

TIP

When it comes to mobile devices, make sure all passwords are unique and that credentials are not openly stored on the device. Avoid public Wi-Fi as malicious networks could give a hacker access to your device.

If you receive an out-of-character message from a contact, let them know as it may be a sign they were hacked. If device compromise occurs, make sure to change all passwords once the device is secure.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Natalia has been saving up to buy a house for years. The time has finally come. After looking online and touring houses in-person, she finally found the one for her. Soon after submitting her offer, she got the news it had been accepted!

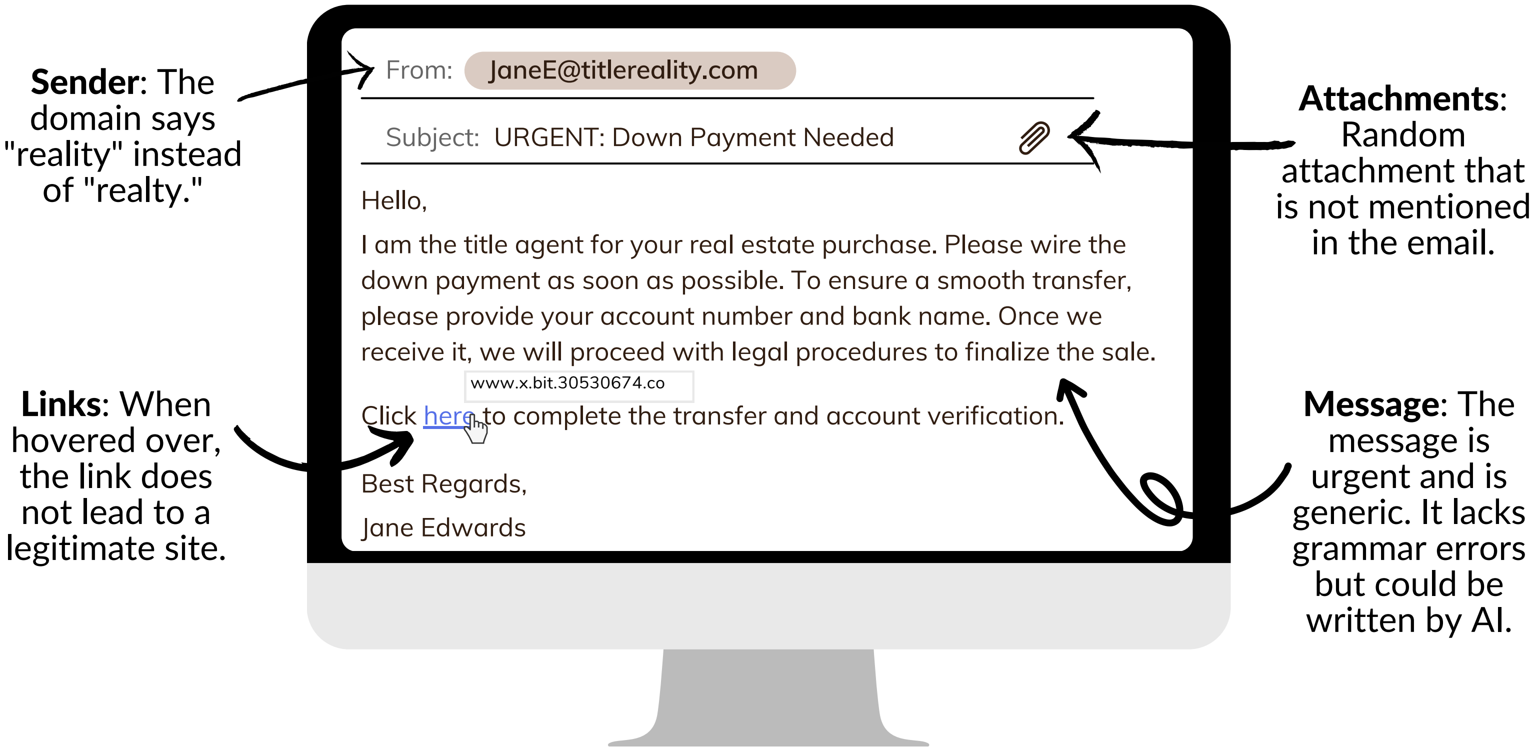
After her offer was accepted, Natalia received an email from a title agent telling her to wire the down payment so they could finalize the sale. Natalia didn't want to slow down the process or jeopardize the sale, so she wired the payment immediately.

A few days later, she received another email from her realtor, and a different title agent named Jane, telling her the date and time of the closing. When she arrived at the closing, Natalia asked if they had received her payment. Her heart dropped when the new title agent told her they had not received any payment. Natalia pulled up the email and Jane told her she had not sent that. Later they found out that Jane's account had been compromised and a cybercriminal was sending fake emails to her clients, pretending to be her.

Business Email Compromise (BEC) Tips

- Especially during exciting times like purchasing a house, make sure to analyze emails before clicking links or sending money.
- Even if a message seems relevant, verify with a known point of contact in-person or through another method.
- Just because a message doesn't fit a "phishy" mold doesn't mean its entirely legitimate.

SLAM Analysis



Sender: The domain says "reality" instead of "realty."

From: JaneE@titlereality.com

Subject: URGENT: Down Payment Needed

Hello,

I am the title agent for your real estate purchase. Please wire the down payment as soon as possible. To ensure a smooth transfer, please provide your account number and bank name. Once we receive it, we will proceed with legal procedures to finalize the sale.

www.x.bit.30530674.co

Click here to complete the transfer and account verification.

Best Regards,

Jane Edwards

Attachments: Random attachment that is not mentioned in the email.

Links: When hovered over, the link does not lead to a legitimate site.

Message: The message is urgent and is generic. It lacks grammar errors but could be written by AI.

THE MONTHLY MASHUP

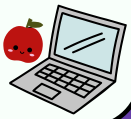
KEY TAKEAWAYS

Taking the time to review the basics could be the difference between staying secure or losing money and data. Always make sure to analyze emails and think twice before clicking.

JOKE OF THE MONTH

Why did the teacher bring her computer to lunch?

Answer: Because it was an apple.

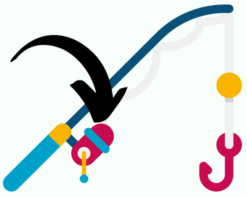


JUNE 29TH: WORK FROM HOME DAY

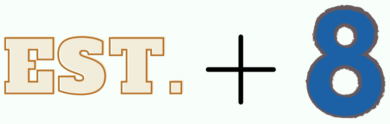
Working from home has its benefits, but it can lead to an increase in device compromise due to a more relaxed mindset in the safety of your own home. Make sure to stay alert when working from home.

PICTURE WORD GAME

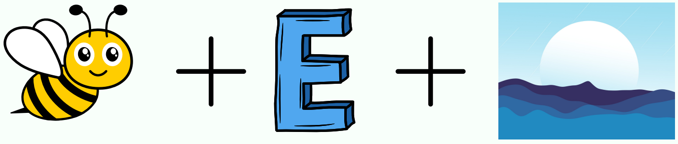
Clue: A new take on a classic scam.



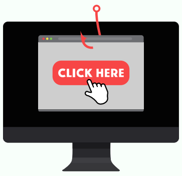
R _ _ l



E _ _ a _ _



_ _ _



S _ _ _

Answer: Real Estate BEC Scam