# THE CLOCK IS TICKING

The time for cybersecurity is now!

## THIS MONTH'S TOPICS:



Whether the past year brought hardship or prosperity, the coming of the new year is always a time to reflect on what is truly important.

As resolutions are being made for 2023, now is the time to think about cybersecurity. From educating others, to gaining a better understanding of the technology we use every day, designating time each day for cybersecurity can make a big difference.

In this month's newsletter, discover the truth about Bluetooth, the post-holiday scams to watch for, and much, much more!

Report Scams

Watch Trainings

Check Privacy Settings

# Cybersecurity RESOLUTIONS

## HELP OTHERS STAY SAFE ONLINE

### Elderly

If your elderly friends and family receive frequent spam calls or emails, they are more prone to scams and may have fallen for one already. Encourage them to ignore unknown callers and to register for the Do Not Call list. Make sure they are also checking their bank accounts for unknown payments. It may be helpful for them to have a trusted contact added to their bank account with view-only privileges to help monitor transactions.

### Coworkers

Cybersecurity in the workplace is becoming a hot topic of office conversation. By asking questions and focusing on the issues your coworkers are facing, your team will be better equipped to face the constant threat of cybercriminals. New scams and breaches happen every day. Bringing up these concerns is a great way to discuss cybersecurity and make it relevant.

### Youth

Children and teens are more connected than ever before. Encourage them to take privacy settings seriously, especially with social media accounts. For younger children, make sure devices have parental controls. When it comes to scams and malware, make sure the kids and teens in your life know to avoid clicking on unknown links or update requests without checking with an adult first.

# BLUETOOTH

## Is it really safe?

### BLUETOOTH EXPLAINED

The convenience and ease of Bluetooth have made it an integral part of society. Bluetooth can pair devices, share files, create hotspots, and more. While features like accepting new connections and distance restrictions do improve the security of Bluetooth, it is still important to stay up to date on Bluetooth attack methods and safety tips.

### HOW TO STAY SAFE

While Bluetooth does pose some security risks, there are many ways to stay safe.

- Turn off Bluetooth when possible.
- Don't allow public pairing.
- Don't share sensitive information over Bluetooth.
- Make sure your device is not discoverable.
- Keep devices updated.

### BLUETOOTH ATTACKS

#### BLUEJACKING

This attack involves one device hijacking another via Bluetooth and sending spam messages. At the least these messages are an annoyance, at most they contain malware.

#### BLUESNARFING

More malicious in nature, Bluesnarfing is when a cybercriminal uses Bluetooth connection to gain access to all personal information and data on a device.

#### BLUEBUGGING

This occurs when a hacker uses a secret Bluetooth connection to access a device. They can monitor activity, see data, and even impersonate the user on the device's apps.

# 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.*

Everything was winding down from the busy holiday season. Shanice had received many gift cards from friends and family, but she noticed that some of them did not have the amounts written on the back, so she turned to the web to check the balance.

She typed "gift card balance checker" into the search engine and scrolled through the results. She ended up choosing a website that offered free gift card balance checks. After clicking on the link, she was taken to a legitimate-looking site.

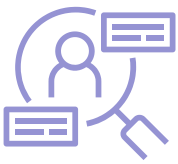
She was prompted to enter the card number and security code. As she entered the information, Shanice had an uncomfortable feeling, so she decided to check some reviews on the website to make sure it was legit.

She soon found that the website had very few reviews. After scrolling through the results, she found some negative comments that said the website was a scam, and that by entering the card information, the scammer would have accessed the remaining gift card balance.


## Did you spot the red flags?

- Even if it appears on a search result, unknown websites with free offers should be treated with caution.
- She did not check the back of the gift card to see if it provided any instructions on how to check the balance.
- Shanice should have checked the reviews first, before entering information on the website.


Only use official websites to check gift card balances. The websites of the gift card brand often include ways to check the balance.



Research the website first. If there are no reviews or if there are signs of a scam, do not enter the website or enter any personal data.


According to consumer reports, $233 million was lost to gift card scams in 2021 and the scammers have certainly not slowed down this past year.


## Key Takeaways

There are many different ways to help those around you stay safe and secure online.

Now is the time to take control of your cybersecurity position.

**Educating friends and family:** People from every generation can benefit from discussing cybersecurity news, enabling online privacy settings, and avoiding calls and emails from unknown users.

**Bluetooth safety:** Bluetooth can be used safely by being aware of common attack methods, monitoring device settings, and avoiding sharing sensitive data.

**Using gifts wisely**: Just because the holidays are winding down, doesn't mean that scammers have stopped. Read reviews before entering gift information or card numbers online.

# Resolutions

A resolution is defined as a firm decision to do something or refrain from doing something. This could mean continuing good practices or changing undesired behaviors.

### How does this relate to cybersecurity?

Making cybersecurity resolutions is a great way to stay on top of digital safety and fix bad cyber habits.

### Now apply this concept to cyber-awareness.

Think about the aspects of cybersecurity you excel in and the areas that need some improvement.

Watch a Micro Training on the topic and make a resolution to improve in that area. Now is the time to take your first step toward reaching your cybersecurity resolutions and goals.