DEPARTMENT OF INFORMATION TECHNOLOGY **Monthly Report**

Cindy Knox, Information Technology Director
(978) 772-8220 ext. 123

Town of Ayer, Massachusetts
1 Main Street – Ayer, MA 01432

REPORT FROM INFORMATION TECHNOLOGY – NOVEMBER 2022

PROJECTS / HARDWARE / SOFTWARE:

- Troubleshoot & resolve issues at Town Hall, DPW, Ayer Fire, and Council on Aging.
- Employee Security Awareness Training.
- Setup new employees: remove access for terminated employees.
- Set up new and replacement computers, phones, tablets, and printers.
- Dispose of old equipment.
- Facilitated 9 Zoom Meetings.

WEBSITE / SOCIAL MEDIA:

- Maintain website and social media
- Monitor Daily
- Add video to the Town's website and social media.
- Minutes, agendas, calendar, and page updates
- Post Notices to Announcements on the Website, Facebook, Twitter, and APAC as needed
- Post updates to the internal and external signage
- Promote local events.

STATISTICS:

Social Media / email:

1. Facebook page reach: 10.2K
2. Twitter followers: 1,491
3. Email subscribers: 4,442

WEBSITE:

1. Top Five Web Pages
    1. Elections
    2. Assessor
    3. Online Payments
    4. Transfer Station
    5. Police Department

2. Number of page views: 26,244
3. Average visit duration: 2 min 7 sec

5 Top Scams to Watch Out for This Holiday Season

By being aware of these five popular scams circulating this holiday season, you can protect yourself and your loved ones from potential fraud.

The holiday season is a time when people are especially vulnerable to scams. This is because they are busy and often have their guard down. Criminals take advantage of this by circulating fake e-gift cards, posing as charities, targeting specific demographics, and so on. In this 3-minute article, we will discuss 'Google's five most popular scams' being circulated this holiday season. So if you want to be aware of the dangers lurking online, then keep reading!

1. E-gift card scams
2. Charities
3. Demographic Targeting
4. Subscription renewals
5. Crypto scams

With the holiday season in full swing, so are gift card and prize scams. These scammers will often lie about being a known contact of yours to try and get you to buy them a gift card, or they may offer an amazing prize in exchange for your credit card information. If you receive any suspicious emails like this from someone claiming to be your friend, make sure to confirm it with them through another method before doing anything further. And as always, if something seems too good to be true, it probably is.

Be wary of scammers and phishing attempts; they actually worsen during the holiday season. This would not only hurt those who fall for the scams, but also charities that could've benefited from donations. For example, an attacker may pretend to be associated with a charity related to current events or one with a familiar name. If someone contacts you asking for money via personal email or another method, beware that it might be fraudulent.

With more people shopping online and sharing personal information this holiday season, scammers are taking advantage by targeting consumers with fraud that seems more realistic. For example, you might get an email from what looks like your child's school PTA about a holiday fundraiser.

But if you click on the link in the email, it could take you to a fake website where you're asked to enter sensitive information like your credit card number or Social Security Number. These types of scams can be difficult to identify because they seem so personalized. But if you're aware of potential threats and know what to look for, you can help protect yourself against them.

Scammers love to target people at the end of the year, and one particularly nasty version of these emails spoofs antivirus services. They lure victims with promises of improved security, but if you take a closer look at the sender's email address, you can usually spot these scams pretty easily.

Cryptocurrency-based scammers are more prevalent during times of higher crypto usage, like now. They often use a cryptocurrency wallet to collect payment and may threaten their victim if they don't receive the funds. Gmail usually sends a warning about these kinds of emails, but it's helpful to know how to spot them on your own too. Some key things to look out for that signal fraud include typos, strange email addresses, and demands for payment.