DEPARTMENT OF INFORMATION TECHNOLOGY

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

Monthly Report

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

Report From Information Technology – January 2023

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 13 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.
- Populate Website with election, town meeting, capital, and budget information.

Statistics:

Social Media / email:

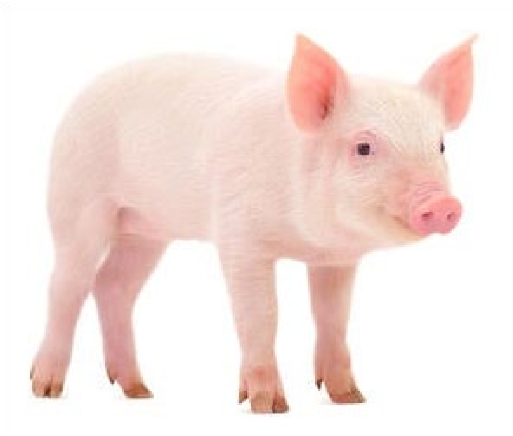
1. Facebook page reach: 7.1K
2. Twitter followers: 1501
3. Email subscribers: 4,583

Website:

1. Top Five Web Pages
    1. Police Department
    2. Assessor
    3. Employment Opportunities
    4. Fire Department
    5. Department of Public Works

2. Number of page views: 32,904
3. Average visit duration: 1 min 35 sec

[Bad Taste] There Is a New Trend in Social Engineering with a Disgusting Name; 'Pig-Butchering'



The technique began in the Chinese underworld, and it amounts to an unusually protracted form of social engineering. The analogy is with fattening up a pig, then butchering it for all it's worth. In this case the analogy is a bit off, since the criminal doesn't really fatten up the pig, not that much, anyway, but it works at least this far: they develop their marks slowly, and they get the marks to fatten up the fraudulent accounts they ultimately drain.

It begins with a cold call, without there necessarily being any other preparation. "Scammers cold-contact people on SMS texting or other social media, dating, and communication platforms," Wired writes. "Often they'll simply say 'Hi' or something like 'Hey Josh, it was fun catching up last week!'"

And an act of common courtesy, telling the caller in effect they've got the wrong number, sets the social engineering in train. "If the recipient responds to say that the attacker has the wrong number, the scammer seizes the opportunity to strike up a conversation and guide the victim toward feeling like they've hit it off with a new friend. After establishing a rapport, the attacker will introduce the idea that they have been making a lot of money in cryptocurrency investing and suggest the target consider getting involved while they can."

Like any classic confidence game, pig-butchering works by developing rapport with the victim. That rapport may be rooted in loneliness (a lot of pig-butchering begins with contact on dating sites) or it may be rooted in a desire for financial gain.

That second motive is often derided as "greed," but that seems unfair–it's as often as not a desire for financial security, and the criminals use the trust the victims develop for them over time to induce them to move funds into bogus financial services accounts that the criminals can eventually access, drain and close out.

"Next, the scammer gets the target set up with a malicious app or web platform that appears trustworthy and may even impersonate the platforms of legitimate financial institutions," Wired explains. "Once inside the portal, victims can often see curated real-time market data meant to show the potential of the investment. And once the target funds their 'investment account,' they can start watching their balance 'grow.'

Read more about this: There is a New Trend in Social Engineering with a Disgusting Name; "Pig-butchering" (knowbe4.com)