frogworks

Managing Your Technology So Your Business Doesn't Croak.

February 2022

Issue 2 Volume 12

Ribb"IT" Review

INSIDE THIS ISSUE:

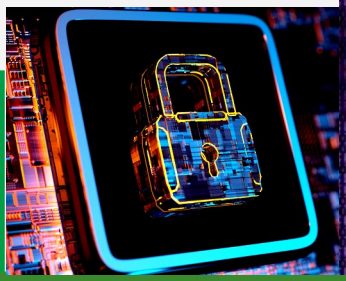
- Falling in Love With Cybersecurity
- Don't Call Me
- Increased Online Love Scams Are Costing Victims Big Money
- Tax Time Brings Out The Hackers

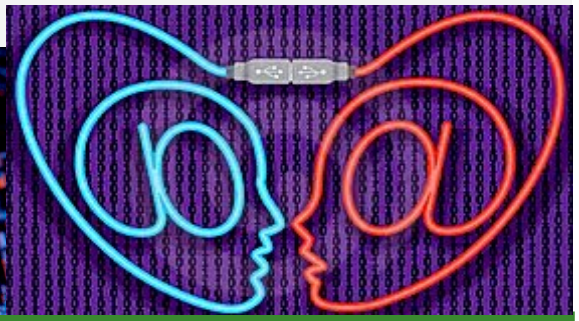
Although there are clear risks with online dating services and applications, these connection tools can still be safe when used properly. Keep your wits about you and always be cautious when things seem too good to be true.

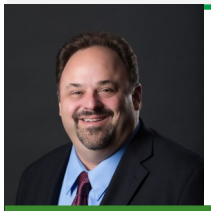
Social Engineering tactics such as pretexting, reciprocity, and authority will continue to be used by successful scammers both on and off dating sites. Know the warning signs and when to slow down the conversation.

Don't get caught in a bad romance. Scammers thrive on dating applications because they can hide behind their fake personas and use social engineering tactics to lure in their victims.

If your not in the market for love right now, you may know someone who is. Pass on your knowledge to others to keep them safe and speak up if something doesn't seem right.







This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Don't Call Me

T-Mobile Reports Scam Calls Have Increased 116 Percent Since 2020

If you're like most cellphone users, you absolutely love the automatic call blocking feature that most companies offer as part of their standard service. A call comes in from a "suspicious" number and the phone just blocks it.

Since those calls are out of sight and out of mind however, it's easy to lose sight of the fact that they're still happening. In fact, according to data recently offered by telecom giant T-Mobile the company has blocked a staggering 21 billion scam, spam, and other unwanted robocalls so far this year.

Even more dismaying though is the fact that this year (2021) has seen scam call traffic jump by an almost unbelievable 116 percent compared with the data from last year. That amounts to more than 425 million scam calls attempted every week. It's a mind-boggling crush of phone traffic thankfully blocked by the fine folks at T-Mobile and other carriers.

These calls run the gamut. According to the company's data the calls were related to a broad range of topics including fake vehicle warranty scams, scams related to the Social Security office, package delivery, and insurance related scams to name a few.

The company had this to say about its "Scam Shield" service:

"T-Mobile Scam Shield has identified or blocked over 21 BILLION calls for T-Mobile and Metro by T-Mobile customers through early December 2021.

The lowest measured month for scam traffic was January 2021, identifying 1.1 billion calls as Scam Likely. By November, volume had increased exponentially, and T-Mobile identified double the January traffic at 2.5 billion calls as Scam Likely."

Telephone Scam tips:

1. Block the numbers.
2. Accidentally Answered? Hang up, Do #1.
3. Don't give your personal or financial information in response to a request that you didn't expect.
4. Join the national Do Not Call Registry that limits the telemarketing calls you receive.

DoNotCall.gov

Don't Be Fooled By Phone-y Calls

Increasing Online Love Scams Are Costing Victims Big Money

Online dating sites have seen a tremendous surge in memberships these past 2 years. Naturally this proved to be an irresistible lure to scammers around the world. So much so that the FBI has recently issued a warning concerning confidence fraud. The surge in these types of scams have very real costs that impact those who fall victim to them in two main ways:

According to FBI statistics these scams have cost their victims more than $113 million since the start of 2021 but the financial cost is just the beginning. Since these scams are designed to play with the emotions of their victims there's a very real emotional cost as well.

To execute the scam the scammers begin by creating fake profiles on online dating websites and begin conversing with potential matches in the dating site's ecosystem.

Once a potential victim is on the hook and lured by the prospect of romance the scammer will invent a story about a sudden crisis. The entire point of the story is to try and convince the victim to part with his or her money.

In terms of protecting yourself against such scams the FBI Advisory recommends the following:

- Never send money, trade, or invest per the advice of someone you have solely met online.
- Do not disclose your current financial status to unknown and un-trusted individuals.
- Do not provide your banking information, Social Security Number, copies of your identification or passport, or any other sensitive information to anyone online or to a site you do not know is legitimate.
- If an online investment or trading site is promoting unbelievable profits, it is most likely that--unbelievable.
- Be cautious of individuals who claim to have exclusive investment opportunities and urge you to act fast.

Tax Time Brings Out the Hackers

It's tax season once again! That, among other things, means that hackers and scammers are out in force, so beware!

As in years past, the primary vehicle hackers and scammers use to run their various tax scams are phishing emails. They're usually designed to appear as though they come from the IRS, and generally indicating that there's some type of problem with your tax record which will delay your refund.

The idea, of course, is to get you worried enough that you'll click on one of the links embedded in the email. The link may look like it's taking you to a page on the IRS.gov website, but is actually a cleverly disguised malicious site controlled by the hackers. Therefore, any information you enter on capture boxes on that site will be given to the hackers themselves.

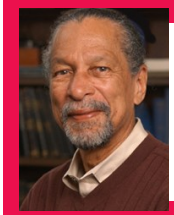
Remember that the IRS will never ask you for any personal information via email and if you suspect that there's a problem with your account, or with the taxes you may have already filed. The best approach is to manually type in the IRS' web address, rather than clicking on any link embedded in an email. Even better, pick up the phone and speak with someone at the IRS directly.

Choose a reputable tool or personal filer to help with taxes. Find a trusted source to help you with your tax filings. Make sure the preparer or tool takes the security of your information seriously.

Report any potential scams to your supervisor and IT when they occur at work. If you've fallen victim outside of work, contact your local consumer protection agency.

Celebrating Black History Month

To celebrate Black History Month, we are honoring a all-stars who positively contribute to improving the culture of cybersecurity.



James Edward Maceo West is an American inventor and acoustician who, in 1962, developed **the foil-electret microphone** used in 90 percent of microphones, that includes cell phones! Fun fact, West home town was Farmville, VA!

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER