February 2021
Issue 2 Volume 11

frogworks
Managing your network so your business doesn't croak.

Run your business without worrying about technology

Ribb"IT" Review

INSIDE THIS ISSUE:

- What's the Deal With Cookies
- 6 Tips to Thwart Covid-19 Cyberscams
- Erasing Your Digital Footprint
- New Paypal Phishing Attempts

What's the Deal With Cookies?

An internet cookie is a website's way of keeping track of its visitors and their activity. As they collect data, cookies can help the website optimize the user's experience with login assistance, advertisement management and preference settings.

Generally, there are no security concerns with these internet cookies BUT their issues relate more to privacy concerns. The good news is, there are ways that you can manage your cookies from your internet browser. Here are some options:

Block Cookies - Your internet browser should have options available to block cookies altogether or block certain types of cookies.

Set Cookie Permissions - Other permissions can be set to reduce and control how cookies are used during your browsing session including restricting specific sites from using cookies.

Clear Cookies - Cookies and other site data can be cleared in your internet browser at any time, or preferences can be set to automatically clear cookies for you when you close your browser.

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

The only way to do great work is to love what you do!

-Steve Jobs

6 TIPS to Thwart COVID-19 Cyberscams

What can you do to help stop online scam artists from taking advantage of the global pandemic? Here are tips to keep you connected—and secure.

#stayingconnected

1 Think Before You Click

- Don't **click on links from sources you don't know**. They could contain viruses.

2 Turn to Official Sources

- Watch for emails claiming to be from public health experts. Here are the official websites of the **Centers for Disease Control and Prevention** and the **World Health Organization**.

3 Vaccine Hoax Alert

- Ignore online or phone offers for vaccinations. There currently are no vaccines or other products—prescription or over-the-counter—that treat or cure COVID-19.

4 Think Before You Give

- Do your homework before giving to **charities** or crowdfunding sites.
- Don't let anyone rush you into making a donation.
- If someone wants donations in cash, by gift card or by wiring money, just say no.

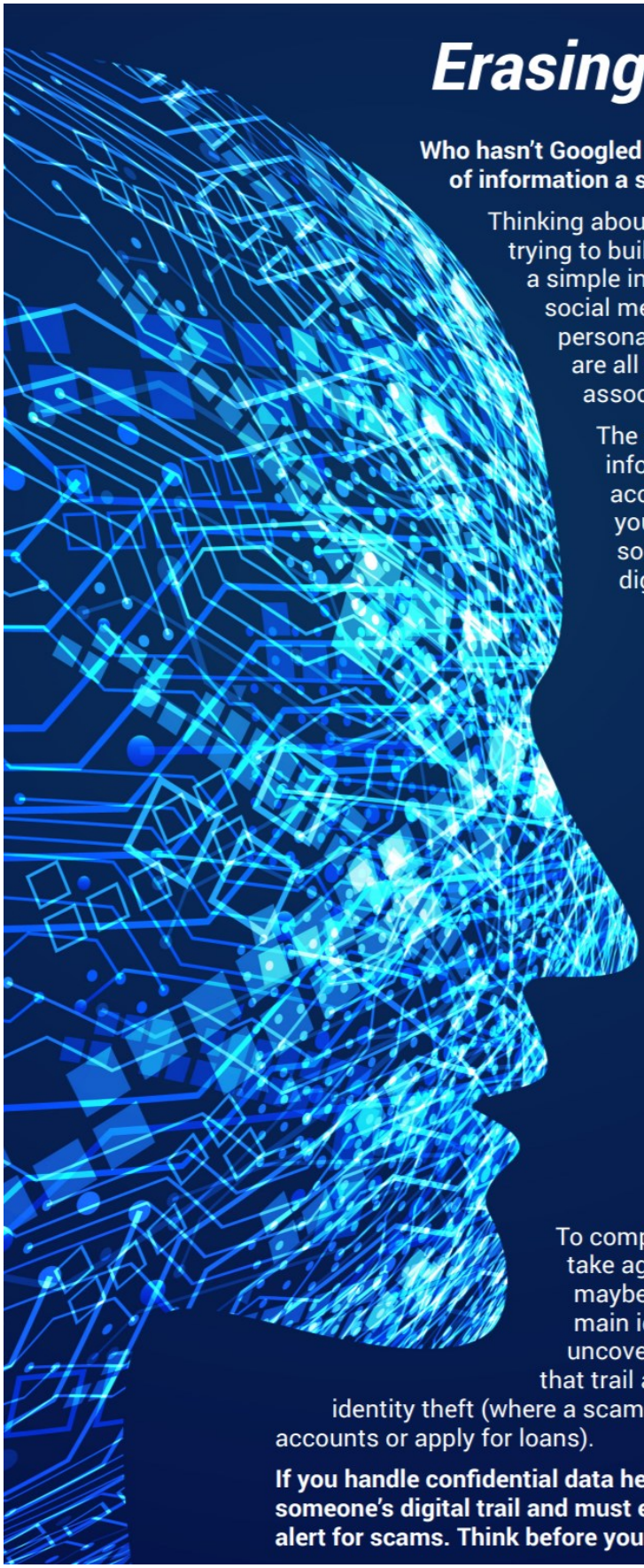
5 Don't Share Personal or Financial Data

- Via email or unsolicited phone call.

6 Turn on Auto Updates

- Keep your software up-to-date on your computer, smartphone and tablet to defend against viruses and hacking attempts.

Erasing Your Digital Footprint



Who hasn't Googled themselves? It's always interesting to find out what kind of information a search engine associates with our name.

Thinking about it from a malicious perspective: if a scammer were trying to build a profile on you, how much data could they get from a simple internet search? Most likely, they would identify which social media sites you've joined; they would know if you have a personal blog; they might even find pictures of your face. These are all part of your digital footprint—a trail of information associated with your internet activity.

The amount of harm this could lead to depends on how much information you allow to be public. If your social media accounts are set to private, scammers won't have access to your friends, family members, or anything you post. Private social media accounts are one way to cover some of your digital footprints. Here are a few others:

- Upgrade privacy settings in your browser so that it doesn't track your location or any web or app activity.
- Limit the amount of information you make public, even if your social media accounts are set to private.
- Where possible, deactivate any accounts you no longer use (looking at you, Myspace).
- Review and revise permissions granted to mobile apps, and delete any apps you no longer need.
- Consider getting a VPN (virtual private network), which drives your internet connection through an encrypted tunnel and prevents anyone from seeing your location or activity.

To completely remove your digital footprint, you will have to take aggressive steps, such as deactivating all accounts and maybe even hiring a firm that specializes in data deletion. The main idea: we all leave behind a trail of data that can easily be uncovered. It's essential to take measures to hide as much of that trail as possible, so it doesn't lead to security incidents like identity theft (where a scammer uses your personal information to open fraudulent accounts or apply for loans).

If you handle confidential data here at work, you become partially responsible for someone's digital trail and must ensure it never gets exposed. Use common sense. Stay alert for scams. Think before you click, and always follow our organization's policies.

New PayPal Phishing Attempts Are After Your Account Info

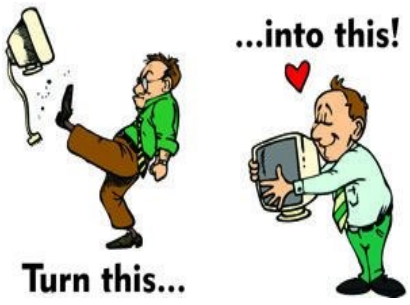
Hackers and scammers have hit the ground running in 2021, launching an extensive new phishing campaign that targets the legions of PayPal users around the world. The campaign is being run on both text message and email channels and if you're a PayPal user, you may have already seen it. If you haven't, in the days and weeks ahead, you'll probably get a text or an email to the effect that the company has detected suspicious activity on your account.

It will say the company has taken the step of "limiting" your account, which puts restrictions on withdrawing, sending or receiving money. Whether you get the text or email variant of the communication, the scammers will "helpfully" include a link, and ask you to verify your account information in order to remove these restrictions.

Naturally, this isn't a legitimate PayPal communication and if you tap or click on the link, you'll be sent to a spoof page that looks like it contains a PayPal login box. Unfortunately, if you attempt to log in, all you'll be doing is handing your login credentials over to the scammers, giving them unfettered access to your account. If you maintain a balance in your PayPal account, it will be promptly drained. If you have bank accounts or credit cards linked to your account, you can expect them to be abused.

This isn't a new idea or a new type of campaign, but it is one of the first coordinated efforts we've seen in 2021 and as such, it pays to be aware of it.

If you get a communication regarding your PayPpal account and you even suspect that it might be true, rather than relying on the link supplied in the text or email, open a new tab and navigate to PayPal's login page manually. That's the easiest way to avoid this type of scam.



Learn to Love your Computer again

this Valentine's Day

With Support from the team

At

frogworks

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

and sign up.

BBB ACCREDITED BUSINESS

We are excited and proud to announce that Frogworks has been accredited by the Better Business Bureau!

WE'VE MOVED!

2670 Crain Highway, Suite 304
Waldorf, MD 20601