Hawaii Association of the Blind Newsletter

March 1, 2024

Upcoming Events

The passing of a member

It is with a heavy heart that we share the news of the passing of Yvette Raposa on February 27, 2024. Our thoughts are with her family during this period of loss.

She was always wanting to help wherever she could and loved connecting with people. Yvette will be missed, but she is now reunited with Michael.

No other information is available at this time.

*** * ***

Next Holoholo Event

When: March 8, 2024

Where: Foodland Farms at Kamakana Ali'i.

The Handi-Van drop off and pick up is at 91-5431 Kapolei Parkway Suite 1704, which is in front of the Foodland Farms. We are meeting from 4:00-7:00 pm.

Anyone is welcome to shop at Foodland Farms and the mall. Encouraging everyone to attend and get familiar with new places, practice mobility skills, learn about accessible apps that may help your shopping and mobility experience.

For more information or to RSVP, please contact Sherrie Martinez at (808) 561-5968.

* * *

Hawaii Association of the Blind Honolulu Holo Holo Shoppers Event

Image Description: Shopping cart filled with fresh fruit

When: Prince Kuhio State Holiday

Tuesday, March 26, 2024, 10am-1pm

Where: Kahala Mall, Meet at Taco Bell/Pizza Hut

Join Certified Orientation & Mobility Specialists

Jeannie Camacho, Sherri Martinez, Amy Downard and Troy Kato

for a supported shopping adventure within a local favorite gathering spot.

Kahala Mall Gift cards are available for shoppers to use during the supported event. White cane skills and route options within the mall will be reviewed.

The purpose of this event is to provide a supported social gathering in a community setting to strengthen shopping, communication and, O&M skills

Please RSVP to Jeannie Camacho, COMS

Email: sixdotscane@gmail.com

Phone: (808)387-1366

* * *

A Skating we will go: Summary of HAB PAY Committee Ice Palace Event.

By Leah Neumann

This past Saturday, February 24th, Hawaii Association of the Blind Parent and Youth committee brought their incredible energy to the Ice Palace, welcoming so many new skaters to the rink! Utilizing Skate-Aids, skating guides, and wheelchairs, we all hit the ice for an unforgettable experience. In our science corner, we explored the fascinating world of friction. Did you know that when skate blades glide over ice, they create heat, melting the ice and creating a nearly frictionless surface? That melted ice then acts as a lubricant, making for smooth sailing on the ice! Stay tuned for more exciting adventures from our next STEAM event!

* * *

What is Phishing?

Phishing is one of the oldest and most common types of cyber fraud. Here's how to protect yourself.

You get an email from a service you use, letting you know that your account is closing. Better click the link before it's gone! Sounds legit, but if you click the link, you could be a victim of one of the oldest and most common cyber scams: phishing. So, what is phishing, exactly?

This type of cyber fraud steals your information or sneaks malicious software (like spyware or ransomware) onto your computer using email as a Trojan horse to violate your online security. The goal of a phishing attack is to fool you into thinking the email is coming from someone you may know, like your bank or employer, and lure you into taking action—click a link or download an attachment—before it's too late.

(Learn about the new form of phishing, quishing which is designed to bypass spam filters.)

Even though phishing is one of the oldest tricks in the book, the techniques used in such messages are becoming more and more sophisticated. That's a frightening prospect—and a good reason to arm yourself with knowledge about the practice in its many forms. We asked cybersecurity experts to not only answer "what is phishing?" but also explain how to avoid falling prey to the scam. There are several strategies, many of which are similar to the steps you'd take if your computer has been hacked or if you're fighting doxxing and attacks on your passwords list.

What is phishing?

"Phishing is a form of social engineering that uses email or malicious websites to either solicit personal information or trick you into downloading malicious software," says Eric Goldstein, executive assistant director for cybersecurity at the Cybersecurity & Infrastructure Security Agency.

Pronounced "fishing," the term evokes the image of an angler throwing a baited hook into the water. In this case, the phishing email is the baited hook, and the scammer behind it is just hoping the target bites. As for the "ph" at the start of the word, it may have been influenced by early hacking terms like phone phreaking (hacking the telephone system).

The practice may have begun on America Online (AOL) in the 1990s, when hackers were trying to trick AOL users into providing their log-in information. Originally, it was a technique for obtaining credit card numbers, but it has grown even more expansive.

These days, when you click on a phishing email, it usually installs a virus or malicious software onto your computer or device. Click it on a work computer or device, and the virus or malicious software can give the attacker access to the company's entire network.

"A typical phishing email will try to engender a sense of urgency or FOMO (fear of missing out) and often makes an offer that seems too good to be true…because it is," says Quentin Hodgson, a senior researcher who focuses on cybersecurity at the Rand Corporation. "How many companies can really afford to give you $300 for your opinion or send you a free iPad?"

Most major data breaches come from phishing emails. The well-known Colonial Pipeline attack from 2021, for example, was a ransomware attack in which criminals got access through phishing emails aimed at a company employee. And the 2014 attack on Sony Pictures was sparked by several emails that appeared to be from Apple, sent to executives of the company.

What are the types of phishing?

By now, you're well past asking, "What is phishing?" The next pressing question is: What forms does phishing take? Hackers can do a lot with just your email, which is probably why email phishing reigns supreme. But there are other ways bad actors use phishing to target us. Once you're aware of the various tactics, you can better avoid them.

Email ph**ishing**

More than 90 percent of all cyberattacks start with a phishing email, says Goldstein. There are three key components of a phishing email that'll fool unsuspecting victims:

• Fake sender: As part of the ruse to trick you into believing a phishing email is legit, attackers make it appear as if the email is from someone you trust, like your credit card company, a government institution, or a retailer like Amazon. It's a shady practice known as spoofing.

• Attention-grabbing subject line: Scammers write email subject lines to get you to open the message.

• Compelling message: The content of a phishing email aims to get you to download an attachment (such as a Microsoft Word file with malicious code in the macros) or click a link that will take you to a malicious site. There, you might inadvertently download malicious software, like adware, spyware, ransomware, or a virus.

Spear phishing

This type of attack targets a specific person or job at a company or organization. Hodgson notes that spear phishing contrasts with a "mass blast" of the same type of email to a whole bunch of recipients over the company's network with the hope of catching a few. Often, a spear-phishing email will target a company's finance department, pretending to be a manager and asking for a large bank transfer right away.

CEO fraud, another type of spear phishing, targets—you guessed it—an organization's CEO. The goal is to get the person in the company's top leadership position to transfer bulk sums of money to the attacker.

Smishing

Smishing refers to SMS phishing, a type of attack in which scammers send SMS text messages to a mobile phone.

This may be the most dangerous form of phishing right now. While people have been aware of email scams since the first “Nigerian prince” sent a request for funds, they may not be as vigilant about phony texts.

Vishing

Most of us are familiar with robocalls—we get enough of them throughout the day. But that’s not the worst thing someone can do with just your phone number.

Worse than telemarketers are the bad guys who use voicemail or a phone call as a phishing attack. In a process known as vishing, a recorded phone call asks you to press a number on your keypad, or a caller fishes for your personal information, maybe saying they’re from the Internal Revenue Service (IRS), your bank, or your child’s school.

Link manipulation

In the world of phishing scams, link manipulation is like hooking a fake worm onto your hook to trick a fish into biting. Except in this case, the worm is a seemingly legitimate link. Hidden beneath it, however, is a link to a malicious website.

Here’s a trick that’ll help you avoid accidentally clicking on a manipulated link: Hover your mouse over the link, but don’t click just yet. Look at the bottom of your web page to see the actual URL you’ll be directed to. If it looks suspicious—say, if the linked text reads “change your Google password” but the URL is http://www.gooooooglepaswrd.com, it’s probably link manipulation.

Clone phishing

Let’s say you recently got an email from your bank with an attachment or a link. Weeks later, you get the same email. Just another case of companies sending way too many emails, right? Maybe not.

With clone phishing, cyberattackers recreate legitimate emails. All of the details are the same, but they replace the links or attachments with phishing content. They figure most people will recognize the email but not look carefully at the changes. And they’re often right.

Malvertising

With a name derived from the words “malicious” and “advertising,” malvertising combines two of your least favorite things: malicious websites and ads. In this type of phishing attack, cybercriminals will email you a fake advertisement that looks legit but contains links to websites that spread malware.

Search engine phishing

This sneaky form of phishing attack targets you when you search. Consider this scenario: You receive a suspicious request for funds on PayPal. Certain it's a scam, you do a Google search for PayPal's contact info. You click a link, unknowingly landing on a phony PayPal website, which delivers you directly into the hands of scammers who will ask for all of your personal information.

That's just one example of a threat called search engine phishing. Using SEO techniques, cybercriminals will get their phishing site to appear on the first page of Google. From there, they can do all sorts of damage: get you to click malicious links, download malware, or ring up one of the bad guys and provide personal information.

Pharming

This type of cyberattack directs traffic from a legitimate website to a fake one. While the site may look legit, it contains malicious material aimed at stealing your personal data.

While data brokers might use cookies and other tools to collect personal info to sell to advertisers, political campaigns, or other interested parties, pharming collects private data with which hackers can steal your identity.

What do phishing emails look like?

There are several ways to spot a phishing email. For starters, look for these features:

- Grammatical errors and misspellings in the message as well as the sender's email address

- Company logos that are not correct

- Links that are malicious (you'll know they're bogus by hovering your mouse over them and reviewing the actual URL)

- A familiar sender (a friend, colleague, or another contact) emailing with a generic or clickbaity subject line, such as "Look what I found," and a link

- A scary subject line

- A subject line offering something for free
- A message that evokes an emotional response or sense of urgency

- Sketchy-looking file attachments

- File-sharing links that require you to enter your password in another window

- A sender who claims to be tech support

Another clue the email you just got is a phishing attack? It's from a government organization like the IRS or Social Security Administration. Legitimate requests from government agencies usually come via mail—rarely email.

Who does phishing target?

We'd all like to think hackers go after the big guys—you know, leaders of giant corporations or influential people in government agencies. But that's not the case. Phishing can target anyone: an online banking customer, a family member using a social network, and even you.

How do I stop phishing emails?

Hackers aren't going to stop sending phishing emails; they're a veritable gold mine. So it's up to you to protect yourself. For starters, follow these important actions:

- Don't click suspicious links or open suspicious email attachments.

- Set good passwords, and don't reuse them across multiple websites.

• Use two-factor authentication to secure your accounts.

• Use spam filters to block emails that can range from annoying to dangerous.

• Avoid posting personal data, such as your date of birth, phone number, address, and vacation plans, on public social media.

• Download an anti-phishing browser extension or security app that protects against phishing attacks.

Avoiding a phishing scam comes down to one major tip, Goldstein says: Take a moment to think before you click.

Sources:

• Eric Goldstein, executive assistant director for cybersecurity at the Cybersecurity & Infrastructure Security Agency

• Quentin Hodgson, senior cybersecurity researcher at the Rand Corporation

• FBI: “Scams and Safety”

• Cybersecurity & Infrastructure Security Agency: “Phishing General Security Postcard”

• Cisco: “Cybersecurity threat trends: phishing, crypto top the list”

• Neural Computing and Applications: “Fighting against phishing attacks: state of the art and future challenges”

• Verizon Business: “The History of Phishing”

* * *

AI-powered robot guide dogs developed for visually impaired

RoboGuide is being tested at the University of Glasgow's James Watt School of Engineering.

By Ryan McDougall

Thursday 08 February 2024 15:05 GMT

The RoboGuide is being developed at the University of Glasgow (University of Glasgow/Chris James/PA)

Blind and partially sighted people may soon be helped to find their way around indoors by robot guide dogs.

Experts from the University of Glasgow are helping to develop the RoboGuide, an AI-powered four-legged robot dog capable of chatting to humans.

The initiative aims to help the visually impaired move more freely around museums, shopping centres, hospitals and other public places.

The robot uses a series of sensors to accurately map and assess its surroundings.

Software developed by the team allows the RoboGuides to learn optimal routes between locations and interpret sensor data in real-time to help it avoid hitting moving obstacles while guiding a human.

They can also understand speech, giving it the ability to provide verbal responses in turn.

Olaoluwa Popoola, of the university's James Watt School of Engineering, is the RoboGuide project's principal investigator.

He said: "Assistive technologies like the RoboGuide have the potential to provide blind and partially sighted people with more independence in their daily lives in the years to come.

"One significant drawback of many current four-legged, two-legged and wheeled robots is that the technology which allows them to find their way around can limit their usefulness as assistants for the visually impaired.

"Robots which use GPS to navigate, for example, can perform well outdoors, but often struggle in indoor settings, where signal coverage can weaken.

"Others, which use cameras to 'see', are limited by line of sight, which makes it harder for them to safely guide people around objects or around bends."

The ongoing development of the RoboGuide was showcased at the university's Mazumdar-Shaw Advanced Research Centre on Thursday.

Developers say the prototype uses a number of cutting-edge technologies, and they aim to have a complete version available in the coming years.

There are an estimated 2.2 billion people in the world living with some form of vision loss, with around two million people in the UK affected.

Professor Muhammad Imran, dean of graduate studies at the James Watt School of Engineering, is co-investigator on the project.

He said: "Our assistive technology project for the visually impaired embodies innovation, fostering inclusivity.

“In Glasgow, we’re pioneering world-changing technologies that hold the potential to transform lives and reshape societal norms.

“This achievement was made possible through collaboration with industry and charity partners and co-creating the design with the invaluable input of end users.”

The Forth Valley Sensory Centre Trust (FVSC) and the Royal National Institute of Blind People (RNIB) Scotland have lent their support to the development of the RoboGuide.

The guide was trialled and tested for the first time with volunteers from both organisations at the Hunterian Museum in Glasgow in December.

The robot helped volunteers find their way around and provided interactive spoken guidance on six different exhibits.

Wasim Ahmad, of the James Watt School of Engineering and another co-investigator on the project, said: “Ultimately, our aim is to develop a complete system which can be adapted for use with robots of all shapes and sizes to help blind and partially sighted people in a wide range of indoor situations.

“We hope that we can create a robust commercial product which can support the visually impaired wherever they might want extra help.”

Jacquie Winning, chief executive of the FVSC, said: “Mobility is a big issue for the blind and partially sighted community.

“RoboGuide is a wonderful solution to that problem, and we are delighted to help test this innovative and creative robot.”

James Adams, director of RNIB Scotland, added: “We’re delighted to be supporting the research and development of technology that could be part of making the world more accessible and empowering blind and partially sighted people to live their lives confidently.”

The nine-month research project has been supported by funding from the Engineering and Physical Sciences Research Council.

* * *