SEPTEMBER 2023

VOL III

DJ'S TECH TIMES

WHAT'S HAPPENING IN IT?

Click It or Phish It? (P. 2)

- Who are this month's winners?
- How are we doing with phishing emails?
- What are the rules for the contest again?

Scam of the Month (P. 3)

- What phishing emails did we fall for?
- What should we watch for in September?

Training Updates (P. 4 & 5)

- What training sessions are available?
- How are we doing with phishing?
- Annual Security Awareness Training

Tip of the Month (P. 6)

- 5 Ways People Get Hacked

Winners!!! (P. 7)

The IT Division has periodically been sending out phishing emails.

These emails need to be reported using the Phish Alert button in your Outlook application.

Successfully reporting the emails as Phishing;
AND not clicking on any links within the email;
AND not replying to the email or interacting with the email in any way.
will result in your name being put in for a drawing!

Five (5) winners will be selected from those who meet the criteria as stated above each month.
For these monthly drawings, prizes will be given out including but not limited to:
·Coffee mugs
·Sweatshirts
·Small kitchen equipment (yogurt maker, casserole dishes)
·Cooler bags
·And more!

For the monthly prizes, you will simply need to report that month's phishing email and not click on any links to be entered into the monthly prize.

Grand Prizes
For the grand prizes, you will need to meet all of the following criteria:
·Not have clicked any links in any phishing emails for the entire year.
·Successfully reported all simulated phishing emails.
·Completed your Annual KnowBe4 Training.
Everyone who fits these criteria will be entered into a drawing for the grand prize: a brand-new e-Bike!

There will be a total of two (2) grand prize winners!
Employees of the IT Division are ineligible for the Click It or Phish It grand prize.

SCAMS OF THE MONTH

From: Human Resources <HR@FDLREZ.COM>
Reply-To: Human Resources <HR@FDLREZ.COM>
Subject: W2 Update

W-2 Update

Denis McDonald,

We are issuing you an amended Form 1040 for the calendar year on behalf of Fond du Lac Reservation. An incorrect employer control number prompted the issuance of this amended form.

If you have already filed with the IRS, you will need to complete and file an additional Form W-2c. The amended Form 1040 can be accessed below and should be reviewed immediately to ensure accuracy.

Amended Form 1040

- HR&FDLREZ.Com is not the email address we would send this from
- Sense of urgency - "should be reviewed immediately"
- Sounds a bit suspicious..."incorrect employer control number" would be worth calling HR before clicking any links
- Hover over the link...it does not take you to the site it claims to.

From: Accounting <Accounting@FDLREZ.COM>
Reply-To: Accounting <Accounting@FDLREZ.COM>
Subject: W2 time -- make sure your info is correct!

To all employees of Fond du Lac Reservation,

Please log in to your employee portal now to make sure that all of information is 100% correct. Corrected W2s are costly and time-cons so help us get it right the first time.

Employee Portal

Thanks!

Accounting Team

- Accounting&FDLREZ.com is a spoofed email address
- "To all employees of Fond du lac Reservation" sounds ambiguous like this email went out to multiple people
- "Take immediate action" again...watch for that!
- Hover over the link!

TRAINING UPDATES

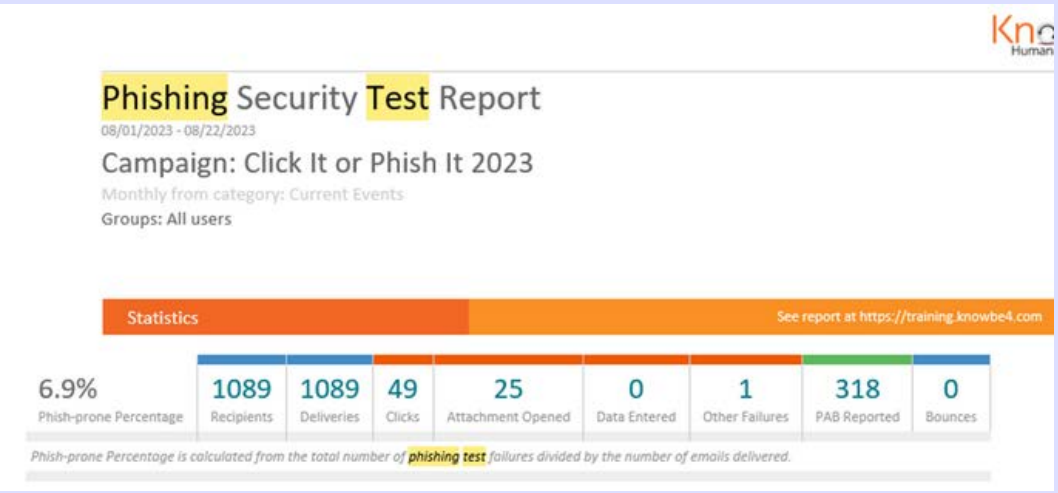
You can earn the badges above by completing training sessions.

Current offerings: Technology 101, Word 101, Excel 101, Outlook 101, iPhone

Coming soon: Word 202, Excel 202, Outlook 202, File Management, Teams

Don't forget you earn additional entries for prizes by completing training!

TRAINING UPDATES



- 49/1089 staff members clicked on our phishing email in August
- 1 person replied - that's still a fail!
- 318 reported
- That results in a 6.9% phish prone percentage for August

Annual Security Awareness Training - Due September 30!

- 579/1135 users completed training - 51%(!)
- 477/1135 users have not yet started - don't be the last one to complete this!

Five Common Ways People Get Hacked

While the intentions of cybercriminals vary, their approach to hacking people tends to follow a few general techniques. Let's review five of the most common ways people are targeted and how you can protect yourself and your organization.

Outdated Devices or Software

Failure to run updates equals failure to patch critical security vulnerabilities. Cybercriminals can use those vulnerabilities to steal valuable information or infect devices with malware. In your personal life, it's best to enable automatic updates whenever available so you never miss an important security patch. At work, follow policy for how and when to install updates.

Phishing Scams

Since phishing scams are the top way people get hacked, they should be your top priority in terms of security awareness. You can spot most attacks by looking for common warning signs. These include suspicious links or unexpected attachments in messages, random requests for confidential information, and threatening or urgent language. Think before you click!

Weak Passwords

Cybercriminals often use password-hacking software that can easily crack weak passwords in minutes, sometimes even seconds. This is how they get access to online accounts, which allows them to steal data or money or leverage social media profiles for malicious purposes. Don't let it happen to you. Ensure every password is several characters long and unique to each account.

Malicious Phone Apps

Popular app stores have implemented rigorous processes to identify and eliminate malicious applications. Unfortunately, it's still common for malicious apps to find their way to the public. Before installing anything, always do some research. Take a few minutes to review how many downloads an app has and ensure the developer is trustworthy. For work-issued devices, never install any software without explicit permission.

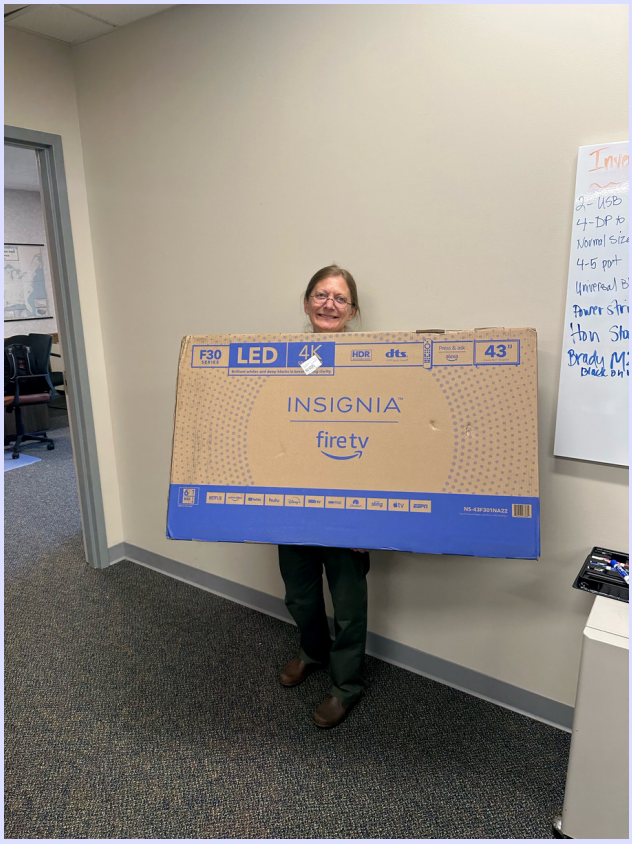
Social Engineering

Not every attack involves sophisticated, technological processes or software. Sometimes, the easiest way to hack someone is by simply misleading them. That's the main idea behind social engineering — the use of deception and psychological manipulation. Avoid this by staying alert, never assuming someone is who they claim to be, and treating any request for money or confidential information with skepticism.

Remember, people (like you) are the last line of defense. Be sure to report suspicious activity immediately, and always follow organizational policies.

And the Winner is...

September Winners:
Jake Kachinske (Operations Manager)
James Barney (Medical Social Worker)
Taylor Shanda (Financial Clerk @ Black Bear)
McKala Crotteau (Mental Health Counselor)
KayLeigh Bushey (Mental Health Practioner)
Jamie Stenberg (Quality Assurance)
Robert Grozdanich (Human Resources)



Jenny Lokken,
Enterprise Accounting

Thank you for reading the Tech Times!
Check back soon for another opportunity to WIN!

Amanda Dornhecker,
Physical Therapy